Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/015085

International filing date: 18 August 2005 (18.08.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-244178
Filing date: 24 August 2004 (24.08.2004)

Date of receipt at the International Bureau: 13 October 2005 (13.10.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００４年　８月２４日
出願番号 Application Number:	特願２００４－２４４１７８
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－２４４１７８
出願人 Applicant(s):	日本電信電話株式会社

２００５年　９月２８日

特許庁長官
Commissioner,
Japan Patent Office

中嶋　誠

【書類名】　特許願
【整理番号】　NTTH165607
【提出日】　平成16年 8月24日
【あて先】　特許庁長官殿
【国際特許分類】　G09C 1/00
【発明者】
【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
【氏名】　堀田　英一
【発明者】
【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
【氏名】　小野　諭
【発明者】
【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
【氏名】　石本　英隆
【発明者】
【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
【氏名】　田倉　昭
【特許出願人】
【識別番号】　000004226
【氏名又は名称】　日本電信電話株式会社
【代理人】
【識別番号】　100083806
【弁理士】
【氏名又は名称】　三好　秀和
【電話番号】　03-3504-3075
【手数料の表示】
【予納台帳番号】　001982
【納付金額】　16,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9701396

【書類名】特許請求の範囲
【請求項１】
所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と通信ネットワークを介して相互に通信可能なイベント順序証明装置が、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明方法であって、
前記利用者装置から前記要求を受信する順序証明要求受信ステップと、
前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算ステップと、
前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約ステップと、
前記順序証明要求集約ステップで生成される順次集約木に関する情報を記憶部に記憶する順次集約木記憶ステップと、
前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、リーフa1のリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、
前記利用者装置ごとに複数の前記登録点に関する情報を前記記憶部に記憶する登録点記憶ステップと、
前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の過去のすべての登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成ステップと、
作成された証明応答を前記利用者装置に送信する証明応答送信ステップと、
を有することを特徴とするイベント順序証明方法。
【請求項２】
所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と通信ネットワークを介して相互に通信可能なイベント順序証明装置が、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明方法であって、
前記利用者装置から前記要求を受信する順序証明要求受信ステップと、
前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算ステップと、
前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約ステップと、
前記順序証明要求集約ステップで生成される順次集約木に関する情報を記憶部に記憶す

る順次集約木記憶ステップと、
前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、リーフa1のリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、
前記利用者装置ごとに前記直前の登録点に関する情報を前記記憶部に記憶する登録点記憶ステップと、
前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の直前の登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成ステップと、
作成された証明応答を前記利用者装置に送信する証明応答送信ステップと、
を有することを特徴とするイベント順序証明方法。
【請求項３】
前記記憶部に記憶される順次集約木に関する情報は、前記順次集約木において割当処理がされた各ノードの位置及び割当値であることを特徴とする請求項１又は２記載のイベント順序証明方法。
【請求項４】
前記記憶部はスタック構造を有し、
第１のスタックは、前記新登録点の即時補完情報を記憶し、
前記利用者装置ごとに具備する第２のスタックは、該利用者装置の遅延補完情報を記憶し、
さらに前記記憶部は前記利用者装置ごとに直前の登録点を記憶する
ことを特徴とする請求項２記載のイベント順序証明方法。
【請求項５】
前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表ステップを有することを特徴とする請求項1乃至４のいずれか1項に記載のイベント順序証明方法。
【請求項６】
前記利用者装置は、前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、イベント順序証明装置の運用中断あるいはデータ消失の時点までに受信し記憶した順序証明応答から、計算可能な割当値を持つ順次集約木のノードのうちで、その親のノードの割当値が計算できないような１つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表手段を有することを特徴とする請求項1乃至5のいずれか1項に記載のイベント順序証明方法。
【請求項７】
前記順序証明要求集約ステップは、前記一定時間間隔終了後に順次集約木のルート値を、次の順次集約木のリーフに割り当てられた新たな登録点の即時補完情報となるように、次の順次集約木のリーフに割り当てることを特徴とする請求項１乃至６のいずれか１項に記載のイベント順序証明方法。
【請求項８】
所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と通信ネットワークを介して相互に通信可能であり、前記利用者装置からの複数の前

記要求に応えて複数の証明書を作成するイベント順序証明装置であって、
前記利用者装置から前記要求を受信する順序証明要求受信手段と、
前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、
前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、
前記順序証明要求集約手段生成される順次集約木に関する情報を記憶部に記憶する順次集約木記憶手段と、
前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、リーフa1のリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、
前記利用者装置ごとに複数の前記登録点に関する情報を前記記憶部に記憶する登録点記憶手段と、
前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の過去のすべての登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成手段と、
作成された証明応答を前記利用者装置に送信する証明応答送信手段と、
を有することを特徴とするイベント順序証明装置。

【請求項9】
所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と通信ネットワークを介して相互に通信可能であり、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明装置であって、
前記利用者装置から前記要求を受信する順序証明要求受信手段と、
前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、
前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、
前記順序証明要求集約手段で生成される順次集約木に関する情報を記憶部に記憶する順次集約木記憶手段と、
前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定

義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、リーフa1のリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、

前記利用者装置ごとに前記直前の登録点に関する情報を前記記憶部に記憶する登録点記憶手段と、

前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の直前の登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成手段と、

作成された証明応答を前記利用者装置に送信する証明応答送信手段と、

を有することを特徴とするイベント順序証明装置。

【請求項１０】

前記記憶部に記憶される順次集約木に関する情報は、前記順次集約木において割当処理がされた各ノードの位置及び割当値であることを特徴とする請求項８又は９記載のイベント順序証明装置。

【請求項１１】

前記記憶部はスタック構造を有し、

第１のスタックは、前記新登録点の即時補完情報を記憶し、

前記利用者装置ごとに具備する第２のスタックは、該利用者装置の遅延補完情報を記憶し、

さらに前記記憶部は前記利用者装置ごとに直前の登録点を記憶する

ことを特徴とする請求項９記載のイベント順序証明装置。

【請求項１２】

前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表ステップを有することを特徴とする請求項８乃至１１のいずれか１項に記載のイベント順序証明装置。

【請求項１３】

前記利用者装置は、前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、イベント順序証明装置の運用中断あるいはデータ消失の時点までに受信し記憶した順序証明応答から、計算可能な割当値を持つ順次集約木のノードのうちで、その親のノードの割当値が計算できないような１つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表手段を有することを特徴とする請求項８乃至１２のいずれか１項に記載のイベント順序証明装置。

【請求項１４】

前記順序証明要求集約手段は、前記一定時間間隔終了後に順次集約木のルート値を、次の順次集約木のリーフに割り当てられた新たな登録点の即時補完情報となるように、次の順次集約木のリーフに割り当てることを特徴とする請求項８乃至１３のいずれか１項に記載のイベント順序証明装置。

【請求項１５】

請求項１乃至７のいずれか１項に記載のイベント順序証明方法の各ステップを前記イベント順序証明装置に実行させることを特徴とするイベント順序証明プログラム。

【請求項１６】

所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、該利用者装置と通信ネットワークを介して相互に通信可能であり、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明装置と、

を備えるイベント順序証明システムにおいて前記証明書の正当性を検証するイベント順序証明検証プログラムであって、

前記イベント順序証明装置は、
前記利用者装置から前記要求を受信する順序証明要求受信手段と、
前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、
前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、
前記順序証明要求集約手段で生成される順次集約木に関する情報を記憶部に記憶する順次集約木記憶手段と、
前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、リーフa1のリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、
前記利用者装置ごとに複数の前記登録点に関する情報を前記記憶部に記憶する登録点記憶手段と、
前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の過去のすべての登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成手段と、
作成された証明応答を前記利用者装置に送信する証明応答送信手段と、
を有し、
前記利用者装置は、
前記要求を前記イベント順序証明装置に送信する要求送信手段と、
前記イベント順序証明装置から前記要求に対する前記証明応答を受信する証明応答受信手段と、
受信した証明応答を記憶する証明応答記憶手段と、
受信し記憶した複数の前記証明書のうち、検証対象の証明書を検証するコンピュータに送信する検証要求手段と、
前記コンピュータから検証結果を受信する検証結果受信手段と、
を有し、
２つの前記利用者装置から検証するそれぞれの１つの前記証明書を受信するか、或いは１つの前記利用者装置から検証する２つの前記証明書を受信する証明書受信ステップと、
受信した各証明書の順次集約木特定情報に基づいて、発行された順序が時間的に前であると判断された証明書を第１の証明書、後であると判断された証明書を第２の証明書とすると、前記第１の証明書を送信した利用者装置に、前記第２の証明書の順次集約木特定情報を送信する順次集約木特定情報送信ステップと、
前記第１の証明書を送信した利用者装置から、前記第１の証明書の前記第２の証明書の発行以降の登録点における遅延補完情報を受信する遅延補完情報受信ステップと、
前記順次集約木の特定のノードに対して、前記第２の証明書に含まれる該ノードの割当値と、前記第１の証明書および前記遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記各証明書の正当性及び前記第１の証明書の登録点が前

記第２の証明書の登録点より時間的に前であることを証明する検証ステップと、
検証した結果を前記２つの或いは１つの利用者装置に送信する検証結果送信ステップと
、
を前記コンピュータに実行させることを特徴とするイベント順序証明検証プログラム。
【請求項１７】
前記利用者装置は、
前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、イベント順序証明装置の運用中断あるいはデータ消失の時点までに受信し記憶した順序証明応答から、計算可能な割当値を持つ順次集約木のノードのうちで、その親のノードの割当値が計算可能できないような１つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表手段、
を有し、
前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、上記利用者装置により上記利用者サイド電子的情報公表手段で割当値が公表されたノードの割当値と、前記証明書受信ステップで受信したデータと前記遅延補完情報受信ステップで受信したデータから該ノード割当値が計算できるときには計算された該ノードの割当値が一致するか否かにより、前記証明書受信ステップで受信したデータと前記遅延補完情報受信ステップで受信したデータが改ざんされていないことの検証を行う利用者サイド公表値による検証ステップを前記コンピュータに実行させることを特徴とする請求項１６記載のイベント順序証明検証プログラム。
【請求項１８】
所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、該利用者装置と通信ネットワークを介して相互に通信可能であり、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明装置と、
を備えるイベント順序証明システムにおいて前記証明書の正当性を検証するイベント順序証明検証プログラムであって、
前記イベント順序証明装置は、
前記利用者装置から前記要求を受信する順序証明要求受信手段と、
前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、
前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、
前記順序証明要求集約手段で生成される順次集約木に関する情報を記憶部に記憶する順次集約木記憶手段と、
前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、リーフa1のリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、
前記利用者装置ごとに前記直前の登録点に関する情報を前記記憶部に記憶する登録点記

憶手段と、
前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の直前の登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成手段と、
作成された証明応答を前記利用者装置に送信する証明応答送信手段と、
を有し、
前記利用者装置の各登録点のうち、前記順次集約木の最も右に割り付けられた登録点を暫定終端点とし、該暫定終端点の割付処理が終了した時点において、所定の登録点の取得可能な補完情報すべてを計算することを、前記所定の登録点の証明書に対するインクリメンタル完全化と定義すると、
前記利用者装置は、
前記要求を前記イベント順序証明装置に送信する要求送信手段と、
前記イベント順序証明装置から前記要求に対する前記証明応答を受信する証明応答受信手段と、
受信した証明応答を記憶する証明応答記憶手段と、
受信し記憶した複数の証明応答のうち、検証対象の証明書に対して前記インクリメンタル完全化の処理を行うインクリメンタル完全化手段と、
インクリメンタル完全化された検証対象の証明書を検証するコンピュータに送信する検証要求手段と、
前記コンピュータから検証結果を受信する検証結果受信手段と、
を有し、
２つの前記利用者装置から検証するそれぞれの１つの前記証明書を受信するか、或いは１つの前記利用者装置から検証する２つの前記証明書を受信する証明書受信ステップと、
受信した各証明書の順次集約木特定情報に基づいて、発行された順序が時間的に前であると判断された証明書を第１の証明書、後であると判断された証明書を第２の証明書とすると、前記第１の証明書を送信した利用者装置に、前記第２の証明書の順次集約木特定情報を送信する順次集約木特定情報送信ステップと、
前記第１の証明書を送信した利用者装置から、前記第１の証明書の前記第２の証明書の発行以降の登録点における遅延補完情報を受信する遅延補完情報受信ステップと、
前記順次集約木の特定のノードに対して、前記第２の証明書に含まれる該ノードの割当値と、前記第１の証明書および前記遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記各証明書の正当性及び前記第１の証明書の登録点が前記第２の証明書の登録点より時間的に前であることを証明する検証ステップと、
検証した結果を前記２つの或いは１つの利用者装置に送信する検証結果送信ステップと
を前記コンピュータに実行させることを特徴とするイベント順序証明検証プログラム。
【請求項１９】
前記利用者装置は、
前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、イベント順序証明装置の運用中断あるいはデータ消失の時点までに受信し記憶した順序証明応答から、計算可能な割当値を持つ順次集約木のノードのうちで、その親のノードの割当値が計算可能できないような１つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表手段、
を有し、
前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、上記利用者装置により上記利用者サイド電子的情報公表手段で割当値が公表されたノードの割当値と、前記証明

書受信ステップで受信したデータと前記遅延補完情報受信ステップで受信したデータから該ノード割当値が計算できるときには計算された該ノードの割当値が一致するか否かにより、前記証明書受信ステップで受信したデータと前記遅延補完情報受信ステップで受信したデータが改ざんされていないことの検証を行う利用者サイド公表値による検証ステップを前記コンピュータに実行させることを特徴とする請求項１８記載のイベント順序証明検証プログラム。

【請求項２０】

所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、該利用者装置と通信ネットワークを介して相互に通信可能であり、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明装置とを備えるイベント順序証明システムにおける前記利用者装置のイベント順序証明検証プログラムであって、

前記イベント順序証明装置は、

前記利用者装置から前記要求を受信する順序証明要求受信手段と、

前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、

前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、

前記順序証明要求集約手段で生成される順次集約木に関する情報を記憶部に記憶する順次集約木記憶手段と、

前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、リーフa1のリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、

前記利用者装置ごとに前記直前の登録点に関する情報を前記記憶部に記憶する登録点記憶手段と、

前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の直前の登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成手段と、

作成された証明応答を前記利用者装置に送信する証明応答送信手段と、

を有し、

前記利用者装置の各登録点のうち、前記順次集約木の最も右に割り付けられた登録点を暫定終端点とし、該暫定終端点の割付処理が終了した時点において、所定の登録点の取得可能な補完情報すべてを計算することを、前記所定の登録点の証明書に対するインクリメンタル完全化と定義すると、

前記要求を前記イベント順序証明装置に送信する要求送信ステップと、

前記イベント順序証明装置から前記要求に対する前記証明応答を受信する証明応答受信ステップと、

受信した証明応答を記憶する証明応答記憶ステップと、

受信し記憶した複数の証明応答のうち、検証対象の証明書に対して前記インクリメンタル完全化の処理を行うインクリメンタル完全化ステップと、
を前記利用者装置に実行させることを特徴とするイベント順序証明検証プログラム。
【請求項２１】
前記インクリメタル完全化は、利用者装置がイベント順序証明装置から受信し記憶した証明応答を用いて、木構造を構成することなく実行されることを特徴とする
請求項１８乃至２０のいずれか1項に記載のイベント順序証明検証プログラム。
【請求項２２】
前記インクリメタル完全化は、
所定の登録点の、前記暫定終端点の割付処理が終了した時点において取得可能な補完情報の各要素に対して、
前記利用者装置がイベント順序証明装置から受信し記憶した１つあるいは複数の証明応答の中から
該要素を直接含むかあるいは該要素を計算するために十分な情報含むような１つの証明応答を選出し、
該証明応答から該要素を計算することにより、
木構造を構成することなく実行されることを特徴とする
請求項２１に記載のイベント順序証明検証プログラム。
【請求項２３】
前記インクリメンタル完全化は、
前記利用者装置の前記暫定終端点より左に位置するすべての登録点に対して行うことを特徴とする請求項２１記載のイベント順序証明検証プログラム。
【請求項２４】
前記暫定終端点の、左に位置する前記利用者装置の登録点a2とその左に位置しa2に最も近い該利用者装置のもう一つの登録点をa1について、
a1の該暫定終端点の割付処理が終了した時点において取得可能な補完情報の全てと、
a2における受理証明書から、a2の該暫定終端点の割付処理が終了した時点において取得可能な補完情報の全てを計算することを完全化波及処理と定義すると、
前記インクリメタル完全化は、
前記暫定終端点の、左に位置し、該暫定終端点に最も近い、前記利用者装置の登録点aに対して該暫定終端点の割付処理が終了した時点において取得可能な補完情報すべてを
前記利用者装置が受信し記憶した証明応答から取得あるいは計算することから始まり、
暫定終端点の左に位置する各登録点の該暫定終端点の割付処理が終了した時点において取得可能な補完情報すべてを計算する処理を、このような登録点のうち一番右に位置する上記登録点aからはじめ、上記完全化波及処理を用いて、順次その左に位置する登録点に対して実行することにより木構造を構成することなく実行されることを特徴とする請求項２３に記載のイベント順序証明検証プログラム。
【請求項２５】
前記インクリメタル完全化は、前記暫定終端点までの各登録点を適宜抽出し、この抽出された登録点間の局所領域に分割し、分割された各局所領域において最も右に割り付けられた登録点を暫定終端点と仮定して、インクリメタル完全化を行うとともに、抽出された各登録点の取得可能な補完情報すべてを計算する方法により行われることを特徴とする請求項１８乃至２４のいずれか1項に記載のイベント順序証明検証プログラム。
【請求項２６】
前記イベント順序証明装置は、
前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表手段を有し、
前記一定時間間隔終了後に、前記所定の登録点に関する情報と前記インクリメンタル完全化ステップで計算された補完情報から、前記順次集約木のルート値を計算するルート値計算ステップと、

電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、
を前記利用者装置に実行させることを特徴とする請求項１８乃至２５のいずれか１項に記載のイベント順序証明検証プログラム。

【書類名】明細書
【発明の名称】イベント順序証明方法、イベント順序証明装置、イベント順序証明プログラム、及びイベント順序証明検証プログラム
【技術分野】
【０００１】
本発明は、デジタル・データの生成を伴うイベントの生起順序を証明するイベント順序証明技術に関する。
【背景技術】
【０００２】
イベント順序証明技術は、デジタル・データの生成を伴う複数のイベントの間の生起順序を証明するとともに、そのようなイベントに伴って生成されたデジタル・データが何であったかを証明する技術である。
【０００３】
近年、インターネット上での電子商取引の活発化や、デジタル文書管理の利用拡大に伴い、「誰が、いつ、とんなデータを生成し、交信したか」を第三者が証明する電子公証の仕組みが必要とされている。電子公証は、送受信者の特定、到達確認、送受信等の前後関係の証明、改ざんの検知、電子文書保管等の機能を具備するものであるが、イベント順序証明技術は、このうち、前後関係の証明及び改ざんの検知の機能を実現するものである。
【０００４】
図53は、このようなイベント順序証明技術を用いたイベント順序証明システムを説明する図である。同図に示すイベント順序証明システム900は、利用者（要求者、検証者）30がイベント順序証明の対象データをイベント順序証明装置10に送信すると、イベント順序証明装置 10が利用者30から要求された対象データに対して受付の順番を示すデータを付したイベント順序受理証明書を生成し、該イベント順序受理証明書を利用者に返信するようになっている。
【０００５】
一般に、イベントの順序証明を行うシステムに対しては、次の要件がある。
【０００６】
第１には、イベント順序証明装置10が、全面的には信頼できないとしても、システム全体としては、高い安全性を確保できることである。
【０００７】
第２には、デジタル・データの出力を伴うようなイベントを生成する情報処理機関が一定期間に取得するイベント順序証明からなるシーケンスについて、該シーケンスに属する任意の２つのイベント順序証明の時間的順序を証明できることである。
【０００８】
第３には、デジタル・データの出力を伴うようなイベントを生成する２つの情報処理機関甲と乙が一定期間に実行する複数のイベント順序証明要求の応答であるイベント順序証明からなる２つのシーケンスについて、これら２つのシーケンスを合併した結果である合併シーケンスに属する任意の２つのイベント順序証明の時間的順序の証明を、甲と乙が、この二者の間で特別な同期手段を講じることなく、実行できることである。
【０００９】
第４には、デジタル・データの出力を伴うようなイベントを生成するイベント順序証明システムの２つの利用者装置甲と乙の各々が取得する２つのイベント順序証明のシーケンスに対して、所定の複数の順序証明要求を所定の方法で集約した集約値を甲のイベント順序証明のシーケンスに基づいて計算すること、及び乙のイベント順序証明のシーケンスに基づいて計算すること、及びこの２つの計算結果が一致することの検証を可能とすることである。このことは、甲の取得するイベント順序証明のシーケンスと乙の取得するイベント順序証明のシーケンスが整合していることを検証するために必要である。
【００１０】
第５には、上記第１及至第４の課題として述べた機能を持つ順序証明システムを、システ

ムを構成する各装置の資源と性能、及び装置間を結ぶネットワークの資源と性能についての種々の条件において、実用的な実現方法を持つことである。具体的には、木構造等の非循環有向グラフを用いて順序証明を行う場合、上記非循環グラフが計算機のメモリに収まらない場合においても実現できるようにスケーラビリティを持って実現するためには、いずれの装置（順序証明装置およびそれを利用する利用者装置）も上記非循環グラフをメモリ上に展開する必要がないような方法で実現することが要求される。また同じくスケーラビリティの観点から、当該の非循環グラフが大きくなっても、順序証明装置とその利用者装置の間の通信量が過大とならないことが要求され、装置間の通信量が当該の非循環グラフのノードの数の対数のオーダで抑えられるならばこの要求は満たされる。一般に、ネットワークで結ばれた計算機システムにより所定の機能を実現するために必要なメモリ量及び装置間の通信量と、個々の装置における処理量はトレードオフの関係にあり、 所定の機能を持つシステムをメモリ量、装置の処理能力、およびネットワークの伝送容量等についての種々の状況化で実用可能とするためには、処理量が実用的な範囲でメモリ量および通信量を小さくする実現方式、及び逆にメモリ量および通信量が実用的な範囲で処理量を小さくする実現方式を提供することが有用である。

【００１１】

イベント順序証明装置 10で発行されたイベント受理証明書は、ＰＫＩ（Public Key Infrastructure；公開鍵基盤）のもとでデジタル署名を偽造防止／証明手段として採用する場合には、一般に、利用者30から送られた対象データに受付の順番を付した署名対象データに対するデジタル署名を含んだイベント順序受理証明書となっている。

【００１２】

このように、イベント順序受理証明書にデジタル署名を含め、イベント順序証明の真正性の主要な根拠としてこのデジタル署名を用いるイベント順序証明システムに関しては、イベント順序証明装置 10の不正に対して対抗策がなくサービスの安全性はイベント順序証明装置の信頼に全面的に依存しているため、上記第１の要件を満たす上で問題がある。

上記の問題に対応して、イベント順序証明の真正性の主要な根拠としてはデジタル署名を用いないイベント順序証明の方法も提案されている。例えば、線形リンキング（Linear Linking Protocol）による方法（例えば、非特許文献１および非特許文献２参照。）は、イベント順序証明装置 10が仮に信頼できないとしても、衝突困難一方向関数の衝突困難性を基礎に高い安全性を確保することが可能となっている方法である。図54は、ＰＫＩに依存しない線形リンキングによるイベント順序証明システムを説明する図である。同図に示すイベント順序証明システム910は、複数の利用者30のイベント順序証明対象データ（ハッシュ値）を相互に関連付けるリンク情報L_nを生成し、リンク情報L_nを含むイベント順序受理証明書を返信するようになっており、各イベント順序受理証明書が、それまでに生成されたすべてのイベント順序受理証明書に依存するようになっている。そして、このリンク情報の一部（L_M, L_N）が定期的にマスメディア等（例えば新聞）に公表されるので、これにより、イベント順序証明装置 10の不正を防止し、結果としてシステム全体の信頼を高めることができるようになっている。

【００１３】

この線形リンキングの方式については、イベント順序証明装置10の不正を検出するために利用者30相互の協力が必要であるという問題点がある。また、２つのイベント順序受理証明書C1とC2の発行順序を検証するためには、C1が発行されてからC2が発行されるまでの間に為された全てのイベント順序証明要求に関する大量のデータを取得する必要があり、上記第５の要件を満たす上で問題がある。さらに、利用者30が取得したイベント順序受理証明書を公表された情報と照合して検証するため、即ち、該イベント順序受理証明書と公表された情報が衝突困難一方向関数をにより所定の方式で関係づけられることを検証するためには、利用者30は、イベント順序証明装置10から、上記リンク情報の一部を公表する２つのタイミングに挟まれた期間に受付けられた全ての順序証明要求の数に比例する大量のデータを取得する必要があり、やはり上記第５の要件を満たす上で問題がある。

この問題を部分的に解決するための方法も提案されている。例えば、非特許文献３および非特許文献４においては、一定期間にイベント順序証明装置10で処理されたイベント順序証明要求をまとめ公表するデータを計算するために、非特許文献１および非特許文献２で使われている線形のリストの代わりに、木構造等の非循環有向グラフを用いることにより、２つのイベント順序受理証明書発行順序を検証するために必要なデータ、および利用者30がイベント順序受理証明書の検証を行うために必要なデータの量を、該一定期間に受付けられるイベント順序証明要求の数に比例する量から、その対数（底2）に比例する量に著しく削減する方法を提案している。

【００１４】

この木構造等の非循環有向グラフを用いる方法は、複数のイベント順序証明を纏める一定の期間が終了し、該纏めたデータを公表し、その期間に発行された各イベント順序証明に対して、該イベント順序証明が上記纏めたデータと衝突困難一方向関数により付けられることを証明するための付加データを、イベント順序証明装置から該イベント順序証明を要求した利用者装置が取得してからのみ、上記の第１及至第４の要件として述べた機能を提供している。従って、上述した従来技術の木構造等の非循環有向グラフを用いる方式では、上記の一定期間が終了するまでは、上記第１及至第４の要件として挙げた機能を提供できないという問題、また一定期間が終了する前に順序証明装置が故障したときにはその故障が回復するまで上記第１及至第４の要件として挙げた機能を提供できないという問題、さらに一定期間が終了する前に順序証明装置が故障し該一定期間に発行した順序証明に関するデータを消失した場合には上記第１及至第４の要件として挙げた機能を永久に提供できなくなるという問題がある。

【非特許文献１】S. Haber and W. Stornetta, How to Time-Stamp a Digital Document, Journal of Cryptology, Vol. 3, No. 2, pp. 99—111, 1991

【非特許文献２】J.-J. Quisquater, H. Massias, J.S. Avila, B. Preneel, B. Van Rompay: Specification and implementation of a timestamping system, Technical Report of Universite Catholique de Louvain, 1999. URL: http://www.dice.ucl.ac.be/crypto/TIMESEC/TR4.tgz

【非特許文献３】A. Buldas、P. Laud, H. Lipmaa and J. Villemson：
Time-stamping with binary linking schemes, in Proceedings of Advances on Cryptology (CRYPTO'98), ed. H. Krawczyk, pp.486—501, Springer-Verlag, 1998

【非特許文献４】A. Buldas、H. Lipmaa and B. Schoenmakers,
Optimally efficient accountable time-stamping, in Proceedings of Public Key Cryptography 2000 (PKC2000), eds. Y. Zheng and H. Imai, pp.293—305, Springer-Verlag, January 2000

【発明の開示】

【発明が解決しようとする課題】

【００１５】

本発明は、上記の問題を解決するためになされたものであり、木構造を用い衝突困難一方向関数の衝突困難性を基礎にイベント順序証明を行うシステムにおいて、複数のイベント順序証明を纏める一定の期間が終了する前であっても、上記の第１及至第４の要件として挙げた機能を提供すると同時に、
上記第１及至第４の課題として述べた機能を持つ順序証明システムを、上記木構造が大きくネットワークが木構造の大きさに比例する通信容量を許容しない場合でも実現できるように、いずれの装置も木構造をメモリ上に展開する必要がなく、順序証明装置とその利用者装置の間の通信量が木構造の高さの対数のオーダで抑えられ、かつ各装置における処理量が実用的であるような実現方式を提供すると同時に、ネットワークが木構造の大きさに比例する通信容量を許容する場合には、各装置における処理量が著しく小さくかつ必要メモリ量および装置間の通信量が実用的であるという意味で上記第５の要件を満たすような、イベント順序証明方法、イベント順序証明システムにおける証明装置、及びイベント順

序証明プログラム、及びイベント順序証明検証プログラムを提供することを目的とする。
【課題を解決するための手段】
【００１６】
上記目的を達成するため、請求項１記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と通信ネットワークを介して相互に通信可能なイベント順序証明装置が、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明方法であって、前記利用者装置から前記要求を受信する順序証明要求受信ステップと、前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算ステップと、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約ステップと、前記順序証明要求集約ステップで生成される順次集約木に関する情報を記憶部に記憶する順次集約木記憶ステップと、前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、リーフa1のリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、前記利用者装置ごとに複数の前記登録点に関する情報を前記記憶部に記憶する登録点記憶ステップと、前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の過去のすべての登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成ステップと、作成された証明応答を前記利用者装置に送信する証明応答送信ステップと、を有することを特徴とする。
【００１７】
請求項２記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と通信ネットワークを介して相互に通信可能なイベント順序証明装置が、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明方法であって、前記利用者装置から前記要求を受信する順序証明要求受信ステップと、前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算ステップと、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約ステップと、前記順序証明要求集約ステップで生成される順次集約木に関する情報を記憶部に記憶する順次集約木記憶ステップと、前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で

定まる前記リーフa1の遅延補完情報を、リーフa1のリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、前記利用者装置ごとに前記直前の登録点に関する情報を前記記憶部に記憶する登録点記憶ステップと、前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の直前の登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成ステップと、作成された証明応答を前記利用者装置に送信する証明応答送信ステップと、を有することを特徴とする。

【００１８】

請求項３記載の本発明は、請求項１又は２記載の発明において、前記記憶部に記憶される順次集約木に関する情報は、前記順次集約木において割当処理がされた各ノードの位置及び割当値であることを特徴とする。

【００１９】

請求項４記載の本発明は、請求項２記載の発明において、前記記憶部はスタック構造を有し、第１のスタックは、前記新登録点の即時補完情報を記憶し、前記利用者装置ごとに具備する第２のスタックは、該利用者装置の遅延補完情報を記憶し、さらに前記記憶部は前記利用者装置ごとに直前の登録点を記憶することを特徴とする。

【００２０】

請求項５記載の本発明は、請求項1乃至４のいずれか1項に記載の発明において、前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表ステップを有することを特徴とする。

【００２１】

請求項６記載の本発明は、請求項1乃至5のいずれか1項に記載の発明において、前記利用者装置は、前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、イベント順序証明装置の運用中断あるいはデータ消失の時点までに受信し記憶した順序証明応答から、計算可能な割当値を持つ順次集約木のノードのうちで、その親のノードの割当値が計算できないような１つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表手段を有することを特徴とする。

【００２２】

請求項７記載の本発明は、請求項１乃至６のいずれか１項に記載の発明において、前記順序証明要求集約ステップは、前記一定時間間隔終了後に順次集約木のルート値を、次の順次集約木のリーフに割り当てられた新たな登録点の即時補完情報となるように、次の順次集約木のリーフに割り当てることを特徴とする。

【００２３】

請求項８記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と通信ネットワークを介して相互に通信可能であり、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明装置であって、前記利用者装置から前記要求を受信する順序証明要求受信手段と、前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順序証明要求集約手段生成される順次集約木に関する情報を記憶部に記憶する順次集約木記憶手段と、前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点か

ら前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフalより右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフalの遅延補完情報を、リーフalのリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、前記利用者装置ごとに複数の前記登録点に関する情報を前記記憶部に記憶する登録点記憶手段と、前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の過去のすべての登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成手段と、作成された証明応答を前記利用者装置に送信する証明応答送信手段と、を有することを特徴とする。

【００２４】

請求項９記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と通信ネットワークを介して相互に通信可能であり、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明装置であって、前記利用者装置から前記要求を受信する順序証明要求受信手段と、前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順序証明要求集約手段で生成される順次集約木に関する情報を記憶部に記憶する順次集約木記憶手段と、前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフalより右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフalの遅延補完情報を、リーフalのリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、前記利用者装置ごとに前記直前の登録点に関する情報を前記記憶部に記憶する登録点記憶手段と、前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の直前の登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成手段と、作成された証明応答を前記利用者装置に送信する証明応答送信手段と、を有することを特徴とする。

【００２５】

請求項１０記載の本発明は、請求項８又は９記載の発明において、前記記憶部に記憶される順次集約木に関する情報は、前記順次集約木において割当処理がされた各ノードの位置及び割当値であることを特徴とする。

【００２６】

請求項１１記載の本発明は、請求項９記載の発明において、前記記憶部はスタック構造を有し、第１のスタックは、前記新登録点の即時補完情報を記憶し、前記利用者装置ごとに具備する第２のスタックは、該利用者装置の遅延補完情報を記憶し、さらに前記記憶部

は前記利用者装置ごとに直前の登録点を記憶することを特徴とする。

【００２７】

請求項１２記載の本発明は、請求項８乃至１１のいずれか1項に記載の発明において、前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表ステップを有することを特徴とする。

【００２８】

請求項１３記載の本発明は、請求項８乃至１２のいずれか1項に記載の発明において、前記利用者装置は、前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、イベント順序証明装置の運用中断あるいはデータ消失の時点までに受信し記憶した順序証明応答から、計算可能な割当値を持つ順次集約木のノードのうちで、その親のノードの割当値が計算できないような１つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表手段を有することを特徴とする。

【００２９】

請求項１４記載の本発明は、請求項８乃至１３のいずれか１項に記載の発明において、前記順序証明要求集約手段は、前記一定時間間隔終了後に順次集約木のルート値を、次の順次集約木のリーフに割り当てられた新たな登録点の即時補完情報となるように、次の順次集約木のリーフに割り当てることを特徴とする。

【００３０】

請求項１５記載の本発明は、請求項１乃至７のいずれか１項に記載のイベント順序証明方法の各ステップを前記イベント順序証明装置に実行させるイベント順序証明プログラムであることを特徴とする。

【００３１】

請求項１６記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、該利用者装置と通信ネットワークを介して相互に通信可能であり、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明装置と、を備えるイベント順序証明システムにおいて前記証明書の正当性を検証するイベント順序証明検証プログラムであって、前記イベント順序証明装置は、前記利用者装置から前記要求を受信する順序証明要求受信手段と、　前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順序証明要求集約手段で生成される順次集約木に関する情報を記憶部に記憶する順次集約木記憶手段と、前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、リーフa1のリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、前記利用者装置ごとに複数の前記登録点に関する情報を前記記憶部に記憶する登録点記憶手段と、前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の過去のすべての登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作

成する証明応答作成手段と、作成された証明応答を前記利用者装置に送信する証明応答送信手段と、を有し、前記利用者装置は、前記要求を前記イベント順序証明装置に送信する要求送信手段と、前記イベント順序証明装置から前記要求に対する前記証明応答を受信する証明応答受信手段と、受信した証明応答を記憶する証明応答記憶手段と、受信し記憶した複数の前記証明書のうち、検証対象の証明書を検証するコンピュータに送信する検証要求手段と、前記コンピュータから検証結果を受信する検証結果受信手段と、を有し、２つの前記利用者装置から検証するそれぞれの１つの前記証明書を受信するか、或いは１つの前記利用者装置から検証する２つの前記証明書を受信する証明書受信ステップと、受信した各証明書の順次集約木特定情報に基づいて、発行された順序が時間的に前であると判断された証明書を第１の証明書、後であると判断された証明書を第２の証明書とすると、前記第１の証明書を送信した利用者装置に、前記第２の証明書の順次集約木特定情報を送信する順次集約木特定情報送信ステップと、前記第１の証明書を送信した利用者装置から、前記第１の証明書の前記第２の証明書の発行以降の登録点における遅延補完情報を受信する遅延補完情報受信ステップと、前記順次集約木の特定のノードに対して、前記第２の証明書に含まれる該ノードの割当値と、前記第１の証明書および前記遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記各証明書の正当性及び前記第１の証明書の登録点が前記第２の証明書の登録点より時間的に前であることを証明する検証ステップと、検証した結果を前記２つの或いは１つの利用者装置に送信する検証結果送信ステップと、を前記コンピュータに実行させることを特徴とする。

【００３２】

ここで、「コンピュータ」とは、検証対象の当事者となっている利用者装置自身も含む意味である。尚、以下の発明においても同様である。

【００３３】

請求項１７記載の本発明は、請求項１６記載の発明において、前記利用者装置は、前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、イベント順序証明装置の運用中断あるいはデータ消失の時点までに受信し記憶した順序証明応答から、計算可能な割当値を持つ順次集約木のノードのうちで、その親のノードの割当値が計算可能できないような１つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表手段を有し、前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、上記利用者装置により上記利用者サイド電子的情報公表手段で割当値が公表されたノードの割当値と、前記証明書受信ステップで受信したデータと前記遅延補完情報受信ステップで受信したデータから該ノード割当値が計算できるときには計算された該ノードの割当値が一致するか否かにより、前記証明書受信ステップで受信したデータと前記遅延補完情報受信ステップで受信したデータが改ざんされていないことの検証を行う利用者サイド公表値による検証ステップを前記コンピュータに実行させることを特徴とする。

請求項１８記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、該利用者装置と通信ネットワークを介して相互に通信可能であり、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明装置と、を備えるイベント順序証明システムにおいて前記証明書の正当性を検証するイベント順序証明検証プログラムであって、前記イベント順序証明装置は、前記利用者装置から前記要求を受信する順序証明要求受信手段と、前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順序証明要求集約手段で生成される順次集約木に関

する情報を記憶部に記憶する順次集約木記憶手段と、前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、リーフa1のリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、前記利用者装置ごとに前記直前の登録点に関する情報を前記記憶部に記憶する登録点記憶手段と、前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の直前の登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成手段と、作成された証明応答を前記利用者装置に送信する証明応答送信手段と、を有し、前記利用者装置の各登録点のうち、前記順次集約木の最も右に割り付けられた登録点を暫定終端点とし、該暫定終端点の割付処理が終了した時点において、所定の登録点の取得可能な補完情報すべてを計算することを、前記所定の登録点の証明書に対するインクリメンタル完全化と定義すると、前記利用者装置は、前記要求を前記イベント順序証明装置に送信する要求送信手段と、前記イベント順序証明装置から前記要求に対する前記証明応答を受信する証明応答受信手段と、受信した証明応答を記憶する証明応答記憶手段と、受信し記憶した複数の証明応答のうち、検証対象の証明書に対して前記インクリメンタル完全化の処理を行うインクリメンタル完全化手段と、インクリメンタル完全化された検証対象の証明書を検証するコンピュータに送信する検証要求手段と、前記コンピュータから検証結果を受信する検証結果受信手段と、を有し、２つの前記利用者装置から検証するそれぞれの１つの前記証明書を受信するか、或いは１つの前記利用者装置から検証する２つの前記証明書を受信する証明書受信ステップと、受信した各証明書の順次集約木特定情報に基づいて、発行された順序が時間的に前であると判断された証明書を第１の証明書、後であると判断された証明書を第２の証明書とすると、前記第１の証明書を送信した利用者装置に、前記第２の証明書の順次集約木特定情報を送信する順次集約木特定情報送信ステップと、前記第１の証明書を送信した利用者装置から、前記第１の証明書の前記第２の証明書の発行以降の登録点における遅延補完情報を受信する遅延補完情報受信ステップと、前記順次集約木の特定のノードに対して、前記第２の証明書に含まれる該ノードの割当値と、前記第１の証明書および前記遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記各証明書の正当性及び前記第１の証明書の登録点が前記第２の証明書の登録点より時間的に前であることを証明する検証ステップと、検証した結果を前記２つの或いは１つの利用者装置に送信する検証結果送信ステップと、を前記コンピュータに実行させることを特徴とする。

【００３４】

請求項１９記載の本発明は、請求項１８記載の発明において、前記利用者装置は、前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、イベント順序証明装置の運用中断あるいはデータ消失の時点までに受信し記憶した順序証明応答から、計算可能な割当値を持つ順次集約木のノードのうちで、その親のノードの割当値が計算可能できないような１つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表手段、を有し、前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、上記利用者装置により上記利用者サイド電子的情報公表手段で割当値が公表されたノードの割当値と、前記証明書受信ステップで受信したデータと前記遅延補完情報受信ステップで受信したデータから該ノード割当値が計算できるときには計算された該ノードの割当

値が一致するか否かにより、前記証明書受信ステップで受信したデータと前記遅延補完情報受信ステップで受信したデータが改ざんされていないことの検証を行う利用者サイド公表値による検証ステップを前記コンピュータに実行させることを特徴とする。

請求項２０記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、該利用者装置と通信ネットワークを介して相互に通信可能であり、前記利用者装置からの複数の前記要求に応えて複数の証明書を作成するイベント順序証明装置とを備えるイベント順序証明システムにおける前記利用者装置のイベント順序証明検証プログラムであって、前記イベント順序証明装置は、前記利用者装置から前記要求を受信する順序証明要求受信手段と、前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順序証明要求集約手段で生成される順次集約木に関する情報を記憶部に記憶する順次集約木記憶手段と、前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記ルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、リーフa1のリーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、前記利用者装置ごとに前記直前の登録点に関する情報を前記記憶部に記憶する登録点記憶手段と、前記利用者装置の新登録点に対して、該新登録点の順次割当データ、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報、並びに新登録点の即時補完情報を備える前記証明書と、前記利用者装置の直前の登録点の新登録点における遅延補完情報と、を併せた証明応答を、前記記憶部に記憶された情報から作成する証明応答作成手段と、作成された証明応答を前記利用者装置に送信する証明応答送信手段と、を有し、前記利用者装置の各登録点のうち、前記順次集約木の最も右に割り付けられた登録点を暫定終端点とし、該暫定終端点の割付処理が終了した時点において、所定の登録点の取得可能な補完情報すべてを計算することを、前記所定の登録点の証明書に対するインクリメンタル完全化と定義すると、前記要求を前記イベント順序証明装置に送信する要求送信ステップと、前記イベント順序証明装置から前記要求に対する前記証明応答を受信する証明応答受信ステップと、受信した証明応答を記憶する証明応答記憶ステップと、受信し記憶した複数の証明応答のうち、検証対象の証明書に対して前記インクリメンタル完全化の処理を行うインクリメンタル完全化ステップと、を前記利用者装置に実行させることを特徴とする。

【００３５】

請求項２１記載の本発明は、請求項１８乃至２０のいずれか1項に記載の発明において、前記インクリメタル完全化は、利用者装置がイベント順序証明装置から受信し記憶した証明応答を用いて、木構造を構成することなく実行されることを特徴とする。

【００３６】

請求項２２記載の本発明は、請求項２１に記載の発明において、前記インクリメタル完全化は、所定の登録点の、前記暫定終端点の割付処理が終了した時点において取得可能な補完情報の各要素に対して、前記利用者装置がイベント順序証明装置から受信し記憶した１つあるいは複数の証明応答の中から該要素を直接含むかあるいは該要素を計算するために十分な情報含むような１つの証明応答を選出し、該証明応答から該要素を計算することにより、木構造を構成することなく実行されることを特徴とする。

【００３７】
請求項２３記載の本発明は、請求項２１記載の発明において、前記インクリメンタル完全化は、前記利用者装置の前記暫定終端点より左に位置するすべての登録点に対して行うことを特徴とする。
【００３８】
請求項２４記載の本発明は、請求項２３に記載の発明において、前記暫定終端点の、左に位置する前記利用者装置の登録点a2とその左に位置しa2に最も近い該利用者装置のもう一つの登録点をa1について、a1の該暫定終端点の割付処理が終了した時点において取得可能な補完情報の全てと、a2における受理証明書から、a2の該暫定終端点の割付処理が終了した時点において取得可能な補完情報の全てを計算することを完全化波及処理と定義すると、前記インクリメタル完全化は、前記暫定終端点の、左に位置し、該暫定終端点に最も近い、前記利用者装置の登録点aに対して該暫定終端点の割付処理が終了した時点において取得可能な補完情報すべてを前記利用者装置が受信し記憶した証明応答から取得あるいは計算することから始まり、暫定終端点の左に位置する各登録点の該暫定終端点の割付処理が終了した時点において取得可能な補完情報すべてを計算する処理を、このような登録点のうち一番右に位置する上記登録点aからはじめ、上記完全化波及処理を用いて、順次その左に位置する登録点に対して実行することにより木構造を構成することなく実行されることを特徴とする。
【００３９】
請求項２５記載の本発明は、請求項１８乃至２４のいずれか1項に記載の発明において、前記インクリメタル完全化は、前記暫定終端点までの各登録点を適宜抽出し、この抽出された登録点間の局所領域に分割し、分割された各局所領域において最も右に割り付けられた登録点を暫定終端点と仮定して、インクリメタル完全化を行うとともに、抽出された各登録点の取得可能な補完情報すべてを計算する方法により行われることを特徴とする。
【００４０】
請求項２６記載の本発明は、請求項１８乃至２５のいずれか１項に記載の発明において、前記イベント順序証明装置は、前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表手段を有し、前記一定時間間隔終了後に、前記所定の登録点に関する情報と前記インクリメンタル完全化ステップで計算された補完情報から、前記順次集約木のルート値を計算するルート値計算ステップと、電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、を前記利用者装置に実行させることを特徴とする。
【発明の効果】
【００４１】
本発明によれば、木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、イベント順序証明要求をまとめた公表データを用いなくてもまたイベント順序証明機関がイベント順序証明要求をまとめた公表データを公表する前に障害などのためにサービスを中断したときでも、イベント順序証明機関から発行されたイベント順序受理証明書の検証を行うことができ、公表期間の途中であってもまたイベント順序証明機関がイベント順序証明要求をまとめた公表データを公表する前に障害などのためにサービスを中断したときでも、利用者間におけるイベント順序受理証明書発行の時間的前後を検証することができる。
【発明を実施するための最良の形態】
【００４２】
以下、本発明の実施の形態を図面を用いて説明する。
【００４３】
＜第１の実施の形態＞
（１－１．システム構成）
図1は、本発明の第１の実施の形態に係るイベント順序証明システム100のシステム構成図である。同図に示すイベント順序証明システム100は、イベント順序証明装置（以下、

証明装置という）1、複数のイベント順序証明利用者装置（以下、利用者装置という）2l（l=A，B，…，N）、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク3を備えており、証明装置1が利用者装置2lからのイベント順序証明要求（以下、証明要求という）に応えて、イベント順序受理証明書（以下、受理証明書という）を含むイベント順序証明応答（以下、証明応答という）を利用者装置2lに返信するようになっている。そして、利用者装置2lは、証明装置1から受け取ったこの複数の証明応答から受理証明書を検証することができるようになっている。

【００４４】

証明装置1は、コンピュータネットワーク3を介して利用者装置2lとデータの送受信を行う送受信部11、利用者装置2lからの証明要求として送信されたデジタル・データを順次集約木を用いてまとめるイベント順序証明要求集約部12、受理証明書を含む証明応答を作成するイベント順序証明応答作成部13、証明装置1が一定期間に発行した複数の受理証明書の内容を集約したデータに対して高強度デジタル署名し、公表データとする高強度デジタル署名作成部14、高強度デジタル署名を付加された公表データを電子的に公表する電子的情報公表部15、及び受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部16を有する構成である。

【００４５】

上述したように、イベント順序証明要求集約部12は、順次集約木を用いてイベント順序証明要求をまとめるが、この順次集約木について図2を用いて説明する。図2は、一定期間（例えば1週間など証明装置1が取り纏めデータを公表するサイクル、順次集約期間という）において、利用者装置2lからの証明要求に含まれるデジタル・データの全部あるいは一部を、所定の順次割当データ計算手順に従って計算した結果であるデジタル・データ（これを順次割当データと呼ぶ；例えば、証明要求に含まれるデジタル・データのハッシュ値）を経時的に順次左側から割り当てる値とする順次集約木の一具体例を示す図である。尚、利用者装置2lからの各証明要求が割り当てられた順次集約木のリーフを登録点ともいう。

【００４６】

順次集約木の各ノード（リーフを除く）に割り当てられる値の計算方法は、以下の通りである。順次集約木の親の割当値は、左側の子の割当値H'と右側の子の割当値H"を連接（ビット列とビット列の結合）し、所定の衝突困難一方向ハッシュ関数hを適用した結果であるハッシュ値を計算することにより求められるものであり、これをh(H‖H")と表す。このようにして下位のレベルの割当値から上位のレベルの割当値を計算して、最終的に最上位のレベル（ルート）の割当値（ルート値）Hを求める。

【００４７】

以下においては、図2に示すように、16のリーフを有する順次集約木の場合について説明する。尚、順次集約木リーフの数や高さは、順次集約期間が終了するまで確定しない。また、順次集約木においては、リーフへの値の割当は左から順次行われ、レベルが0より大きいノード（即ちリーフではないノード）に対する値の割当は、それが可能になったときにインクリメンタルに行われる。従って、図2の同一の縦線上にある複数のノードに対しては、値の割当が同一の処理単位の中でほぼ同時に行われる。

ここで、順次集約木のレベルj、番号iのノードを(j，i)、(j，i)の割当値をV(j，i)と表して、図2に示す具体例を説明する。

【００４８】

今、順次集約木リーフに割り当てるハッシュ値がV(0，5)であるとき（登録点が(0，5)であるとき）、このハッシュ値V(0，5)からルート値H（＝V(4，0)）を求めるには、V(0，5)にV(0，4)を左から連接して、ハッシュ値h1'を計算し、該ハッシュ値h1'にV(1，3)を右側から連接してハッシュ値h2'を計算し、該ハッシュ値h2'にV(2，0)を左側から連接してハッシュ値h3'を計算し、さらに該ハッシュ値h3'にV(3，1)を右側から連接してハッシュ値H（＝V(4，0)）を計算すればよい。このような手順によりV(0，5)とそれを補完するデータ（こ

こではV(0，4)，V(1,3)，V(2,0)，V(3,1)）からルート値Hが計算できるとき、V(0，5)はハッシュ関数hによりルート値Hにリンクするという。また、順次集約木におけるV(0,5)の補完データ（以下、順次集約補完データという）は、

［(V(0,4)，L)、(V(1,3)，R)、(V(2,0)，L)、(V(3,1)，R)］

となる。ここで、L及びRは、各々、２つのデジタル・データを連接する際に左から連接こと、及び右から連接することを表す。

【００４９】

イベント順序証明応答作成部13は、図3に示すような受理証明書 EOC(y)を含む証明応答を作成し、利用者装置21に送信するようになっている。同図によれば、受理証明書 EOC(y)は、利用者から送付されたデジタル・データy、上述した順次割当データ計算手順によりデジタル・データyから計算された順次割当データz、順次割当データzが割当てられた順次集約木を一意に特定できる順次集約木番号、順次割当データzが割当てられた順次集約木リーフを一意に特定できる順次集約木リーフ番号、およびその時点で取得できる順次集約補完データの一部（これを登録点の即時補完データと言う） SKの位置情報及び割当値を含むように構成されている。

【００５０】

また、同図によれば、証明応答には、利用者装置21の過去の各登録点の遅延補完データTKの位置情報及び割当値も含むように構成されている。尚、遅延補完データTKとは、当該の証明応答発行後に取得できる順次集約補完データをいい、例えば、図2の具体例においては、V(0,5)にとって、V(2,0)、V(0,4)は即時補完データであるが、V(1,3)、V(3,1)はV(0，15)が割当られた時点以降に取得可能な遅延補完データである。また、一般に、あるリーフa1とそれより右に位置するもう一つのリーフa2において、リーフa2の割当処理が終了した時点で定まるリーフa1の遅延補完データを、a1のa2における遅延補完データという。図２の具体例においては、ノード(0,5)のノード(0,10)における遅延補完データは、ノード(1,3)である。

【００５１】

ここで、本実施の形態における証明応答の具体例を図4を用いて説明する。尚、以下においては、本実施の形態における証明応答の形式を「シーケンス補完方式」と呼ぶ。今、ある利用者装置21からの登録点がX1（ノード(0，2)），X2（ノード(0，11)），X3（ノード (0，18)），X4 （ノード(0，21)），X5 （ノード(0，29)），X6（ノード (0，31)）であるとする。

【００５２】

シーケンス補完の方式においては各登録点において以下のようなデータが利用者装置21に返されるようになっている。

【００５３】

（１）X1点における証明応答には、X1点の即時補完データが返される（具体的には、ノード(1,0)の割当値）。

【００５４】

（２）X2点における証明応答には、X2点の即時補完データ、及びX1点のX2点における遅延補完データが返される（具体的には、X2点の即時補完データとして、ノード(3,0)，ノード(1,4)，ノード(0,10)の割当値、X1点のX2点における遅延補完データとして、ノード(0,3)，ノード(2,1)）の割当値。

【００５５】

（３）X3点における証明応答には、X3点の即時補完データ、並びにX1点及びX2点のX3点における遅延補完データが返される（具体的には、X3点の即時補完データとして、ノード(4,0)，ノード(1,8)の割当値、 X1点のX3点における遅延補完データとして、ノード(0,3)，ノード(2,1)，ノード(3,1)の割当値、 X2点のX3点における遅延補完データとして、ノード(2,3)の割当値）。

【００５６】

（４）X4点における証明応答には、X4点の即時補完データ、並びにX1点、X2点及びX3点の

X4点における遅延補完データが返される（具体的には、X4点の即時補完データとして、ノード(4,0)，ノード(2,4)，ノード(0,20)の割当値、X1点のX4点における遅延補完データとして、ノード(0,3)，ノード(2,1)，ノード(3,1)の割当値、X2点のX4点における遅延補完データとして、ノード(2,3)の割当値、X3点のX4点における遅延補完データとして、ノード(0,19)の割当値）。

【００５７】

以下、X5及びX6においても同様である。このように、シーケンス補完方式においては、証明応答として、ある登録点に関して、該登録点の即時補完データ及びある登録点より前に登録された各登録点の該登録点における遅延補完データが含まれるようになっている。尚、各証明応答は、利用者装置21ごとに管理されるようになっている。

【００５８】

利用者装置21は、コンピュータネットワーク3を介して証明装置1とデータを送受信する送受信部21、所定のデジタル・データを含む証明要求を複数回行うイベント順序証明要求証部22、証明要求に対する証明応答に含まれた受理証明書を検証するイベント順序証明検証部23、受理証明書を含む証明応答をはじめとしてイベント順序証明に関する情報を記憶する記憶部24を有する構成である。

【００５９】

ここで、イベント順序証明検証部23は、受理証明書に対して以下の検証機能を備える。

【００６０】

第１の検証機能としては、証明装置1のデジタル署名作成部14及び電子的情報公表部15を介して公表される公表情報に、受理証明書に含まれる順次割当データがハッシュ関数を介してリンクすることを検証するものである。具体的には、順次集約木のルート値として公表された値と利用者装置21で計算されたルート値が一致するか否か検証するものである。

【００６１】

第２の検証機能としては、公表情報が公開される前であっても、利用者装置21の後述する動作により、利用者装置21間における受理証明書発行の時間的前後を検証するものである。

【００６２】

以下、第２の検証機能を図5を用いて説明するが、その前に、合流点及び認証点の説明をする。

【００６３】

ある順次集約木のリーフaに対して、aからルートに至るパスをaのルート・パスと呼び、rtPath(a)と書く。また、rtPath(a)に属するノードのルート以外のものの兄弟ノード(sibling node)からなるノードの並びを認証パスと呼びauthPath(a)と書く。

【００６４】

このとき、ある順次集約木の２つのリーフa1とa2について、a1より右にa2が位置するとき、a1からルートに至るパスとa2からルートに至るパスの合流する点を、a1とa2の合流点と呼び、合流点のレフト・チャイルド（左側の子）をa1のa2による認証点と呼ぶ。例えば、図4において、登録点X1の登録点X2による認証点は(3，0)の点であり、登録点X2の登録点X3による認証点は(4，0)の点である。

【００６５】

今、２つの利用者装置2A及び2Bが、それぞれ、シーケンス補完方式により、各登録点の証明応答を取得するものとし、図５に示すa，a_1，a_2，a_fを利用者装置2Aの登録点、bを利用者装置2Bの登録点とする。尚、a_fは、暫定終端点と呼ばれるもので、利用者装置2Aの登録点のうち、最も右に位置する登録点である。図５においては、利用者装置2Aの１つの登録点aがあり、それより右に位置する利用者装置2Bの登録点bがあり、さらにその右に位置する利用者装置2Aの登録点a_fがある。

【００６６】

ここで、シーケンス補完方式においては、一般に、登録点aが登録点bより左に位置す

る場合、認証点のラベル（割当値）は登録点bの証明応答（即時補完データ）に含まれており、また、登録点bにおけるイベント順序証明処理が終了した時点以降（例えば、登録点a_1の時点）においては、登録点aの遅延補完データから計算できるラベルには、認証点のラベルが含まれるので、登録点aの登録点a_1における遅延補完データから計算される認証点の割当値と、登録点bの即時補完データに含まれる認証点の割当値が一致するか否かを検証することにより、登録点aと登録点bの時間的前後を検証することができる（詳しくは、後述の順次集約木の性質の項目(3)を参照）。

【００６７】

従って、図５の場合、登録点a_1を現時点としたときの現時点順次集約木における、登録点a の 登録点bによる認証点oの割当値V(o)が一致すれば、登録点ａの登録が登録点ｂの登録より前に起こったことを客観的に証明することができる。イベント順序証明検証部23は、このことを後述する動作により検証するものである。

【００６８】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（CPU：Central Processing Unit）、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置（メモリ）、ハードディスク（HD）等の電源断時にもデータを記憶し続けることができる２次記憶装置を有する電子的な装置から構成されている。このうち、証明装置1のイベント順序証明要求集約部12、イベント順序証明応答作成部13、デジタル署名作成部14及び電子的情報公表部15、並びに利用者装置21のイベント順序証明要求部22及びイベント順序証明検証部23の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、証明装置1の記憶部16及び利用者装置21の記憶部24は、上記主記憶装置あるいは２次記憶装置の機能を備えたものである。

【００６９】

（１－２．システム動作）

次に、以上の構成を有するイベント順序証明システム100におけるイベント順序証明方法、およびイベント順序証明検証方法を図6乃至8を用いて説明する。ここで、図6は、１つの順次集約期間において証明装置1が受理証明書を含む及び証明応答を作成する動作を説明するシーケンス図であり、図7及び8は、利用者装置21が受理証明書に対して第2の検証を行う動作を説明するシーケンス図である。

【００７０】

まず、図６を参照して、イベント順序証明方法について説明する。

【００７１】

利用者装置21が証明装置1にデジタル・データｙ を含む証明要求を送信すると、証明装置1は送受信部11を介して、該デジタル・データｙを含む証明要求を受信する（ステップＳ10，Ｓ20）。

次に、イベント順序証明要求集約部12が、デジタル・データｙ を入力の一部あるいは全部として順次割当データzを計算し、該順次割当データzを順次集約木リーフに割り当てて、インクリメンタルに順次集約木を構成していくとともに、イベント順序証明応答作成部13は、受理証明書を含む証明応答（シーケンス補完の方式；登録点の即時補完データ及び登録点より前に登録された各登録点の該登録点における遅延補完データ）を作成し、送受信部11を介して利用者装置21に証明応答を送信する（ステップＳ30，Ｓ40，Ｓ50）。

【００７２】

これにより、利用者装置21は、受理証明書を含む証明応答を取得することができる（ステップＳ60）。そして、利用者装置21は、このステップＳ10及びＳ60の証明要求送信及び証明応答受信を繰り返す。

【００７３】

一方、証明装置1では、順次集約のための一定期間（順次集約期間）内においては、上述した証明装置1の動作は繰り返され、順次集約期間が終了すると、電子的情報公表部17は、順次集約木のルート値を計算し、このルート値を電子的に公表する（ステップＳ70，Ｓ80，Ｓ90）。

【００７４】
次に、図7を参照しながら、イベント順序証明検証方法について説明する。これは、利用者装置2Iの第２の検証機能に相当するものである。尚、図7は、利用者装置2Aと2B間のデータのやりとりを示すものであるが、利用者装置2Aが利用者装置2Bに後置点判定要求（利用者装置2Aが受け取った受理証明書の登録点より時間的に後の受理証明書に対する順序判定を利用者装置2Bに要求する）行うものである。
【００７５】
まず、利用者装置2Aは、検証したい受理証明書EOC(a)（登録点aにおける受理証明書）を付けて後置点判定要求を利用者装置2Bに送信する（ステップS110）。後置点判定要求を受信した利用者装置2Bは、受け取った受理証明書EOC(a)からリーフ番号n(a)を抽出し、リーフ番号n(a)より大きなリーフ番号を利用者装置2Bの登録点の中から検索する（ステップS120,S130）。リーフ番号n(a)より大きなリーフ番号が利用者装置2Bの登録点にある場合には、該登録点の一つbを選び、そのリーフ番号n(b)を利用者装置2Aに送信する（ステップS140,S150）。これに対して、リーフ番号n(a)より大きなリーフ番号が利用者装置2Bの登録点にない場合には、比較可能データなしの旨のメッセージを利用者装置2Aに送信する（ステップS142）。
【００７６】
リーフ番号n(b)を利用者装置2Bから受信した利用者装置2Aは、リーフ番号n(b)より大きなリーフ番号を持つ利用者装置2Aの暫定登録点a_1を選び、登録点aの暫定終端点a_1における遅延補完データlateData（a,a_1）を取得し、利用者装置2Bに送信する（ステップS160,S170,S180,S190）。尚、比較可能データなしの旨のメッセージを利用者装置2Bから受信したときは、検証を終了する（ステップS144）。
【００７７】
利用者装置2Aから遅延補完データlateData（a,a_1）を受信した利用者装置2Bは、リーフ識別番号n(a)とn(b)から登録点aの登録点bに対する認証点oを計算し、受け取った受理証明書EOC(a)と遅延補完データlateData（a,a_1）から認証点の割当値を計算する（ステップS210）。次に、登録点bの受理証明書EOC(b)に含まれる即時補完データに上記計算で求めた認証点の割当値が含まれているか否かを検証し、認証点の割当値が含まれているときは、登録点aが登録点bより時間的に前に登録されたという判定結果を利用者装置2Aに送信する（ステップS220,S230）。一方、認証点の割当値が含まれていないときは、登録点aが登録点bより時間的に前に登録されたことを証明できず、何らかの不正があるという判定結果を利用者装置2Aに送信する（ステップS220,S240）。
【００７８】
この結果、利用者装置2Aは、判定結果を受信し、取得するので、２利用者間において受理証明書発行の時間的前後を検証することができる（ステップS250,S260）。
【００７９】
尚、上述したイベント順序証明検証方法は、利用者装置2Aが利用者装置2Bに後置点判定要求行うものであったが、前置点判定要求（利用者装置2Aが受け取った受理証明書の登録点より時間的に前の受理証明書に対する順序判定を利用者装置2Bに要求する）を行うようにしてもよい。図8は、利用者装置2Aが利用者装置2Bに前置点判定要求行う場合の利用者装置2Aと2B間のデータのやりとりを示すシーケンス図である。
【００８０】
まず、利用者装置2Aは、検証したい受理証明書EOC(a)（登録点aにおける受理証明書）を付けて前置点判定要求を利用者装置2Bに送信する（ステップS310）。前置点判定要求を受信した利用者装置2Bは、受け取った受理証明書EOC(a)からリーフ番号n(a)を抽出し、リーフ番号n(a)より小さいリーフ番号、及びリーフ番号n(a)より大きいリーフ番号を利用者装置2Bの登録点の中から検索する（ステップS320,S330）。リーフ番号n(a)より小さいリーフ番号及びリーフ番号n(a)より大きいリーフ番号が利用者装置2Bの登録点にある場合には、リーフ番号n(a)より小さいリーフ番号の登録点bを選ぶとともに、リーフ番号n(a)より大きいリーフ番号の暫定登録点b_1を選ぶ（ステップS340,S350）。尚、該当する登録点

がない場合には、比較可能データなしの旨のメッセージを利用者装置2Aに送信する（ステップS342）。そして、利用者装置2Aは、比較可能データなしの旨のメッセージを利用者装置2Bから受信したときは、検証を終了する（ステップS344）。

【００８１】

次いで、利用者装置2Bは、登録点bの暫定登録点b_fにおける遅延補完データlateData（b，b_f）を取得し、リーフ識別番号n(a)とn(b)から登録点aの登録点bに対する認証点oを計算し、受理証明書EOC(b)と遅延補完データlateData（b，b_f）から認証点の割当値を計算する（ステップS360，S370）。次に、登録点aの受理証明書EOC(a)に含まれる即時補完データに上記計算で求めた認証点の割当値が含まれているか否かを検証し、認証点の割当値が含まれているときは、登録点aが登録点bより時間的に後に登録されたという判定結果を利用者装置2Aに送信する（ステップS380，S390）。一方、認証点の割当値が含まれていないときは、登録点aが登録点bより時間的に後に登録されたことを証明できず、何らかの不正があるという判定結果を利用者装置2Aに送信する（ステップS380，S400）。

【００８２】

この結果、利用者装置2Aは、判定結果を受信し、取得するので、２利用者間において受理証明書発行の時間的前後を検証することができる（ステップS410，S420）。

【００８３】

尚、上述したイベント順序証明検証方法は、利用者装置2A及び利用者装置2Bが受理証明書発行の時間的前後を検証したものであったが、本発明はこれに限定されず、当事者以外の第３者機関が検証を行ってもよい。この場合には、利用者装置2A及び利用者装置2Bが検証に必要な情報を第３者機関に送信し、第３者機関が検証を行うものである。

【００８４】

従って、第１の実施の形態のイベント順序証明システム100によれば、木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、利用者装置21から証明要求を受付けた証明装置1が、該証明要求に対して受理証明書を含むシーケンス補完方式（登録点に関して、該登録点の即時補完データ及び該登録点より前に登録された各登録点の該登録点における遅延補完データを証明応答に含む）による証明応答を発行し、利用者装置21がこの証明応答を用いて、利用者装置21間における受理証明書発行の時間的前後を検証することができるので、証明要求をまとめた公表データが電子的に公表される前であっても、受理証明書の正当性を検証することができる。

【００８５】

＜第２の実施の形態＞

（２－１．システム構成）

図9は、本発明の第2の実施の形態に係るイベント順序証明システム200のシステム構成図である。同図に示すイベント順序証明システム200は、証明装置4、複数の利用者装置5l（l=A，B，…，N）、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク3を備えており、証明装置4が利用者装置5lからの証明要求に応えて、受理証明書を含む証明応答を利用者装置5lに返信するようになっている。そして、利用者装置5lは、証明装置4から受け取ったこの複数の証明応答から受理証明書を検証することができるようになっている。

【００８６】

ここで、本実施の形態と第1の実施の形態とは、証明応答の形式が異なるものであり、本実施の形態では、「シーケンス補完方式」とは別の後述する「連鎖補完方式」により証明応答が作成されるようになっている。これは、上述したシーケンス補完方式においては、各利用者装置21の各登録点において、当該の利用者装置21の過去の登録点全てに対してその遅延補完データを当該の利用者装置21に返送しなければならないため、過去の登録点が増加するのに比例して、証明応答のデータ量が増加するが、本実施の形態の連鎖補完方式においては、証明応答のデータ量の増加が抑制されるようになっている。尚、本実施の形態においては、上記実施の形態と異なる構成及び機能を説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

【００８７】
証明装置4は、コンピュータネットワーク3を介して利用者装置51とデータの送受信を行う送受信部11、利用者装置51からの証明要求として送信されたデジタル・データを順次集約木を用いてまとめるイベント順序証明要求集約部12、受理証明書を含む証明応答を作成するイベント順序証明応答作成部41、証明装置4が一定期間に発行した複数の受理証明書の内容を集約したデータに対して高強度デジタル署名し、公表データとする高強度デジタル署名作成部14、高強度デジタル署名を付加された公表データを電子的に公表する電子的情報公表部15、及び受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部42を有する構成である。

【００８８】
イベント順序証明応答作成部41は、図10に示すような受理証明書 EOC(y)を含む証明応答を作成し、利用者装置51に送信するようになっている。同図によれば、受理証明書 EOC(y)は、利用者から送付されたデジタル・データy、上述した順次割当データ計算手順によりデジタル・データyから計算された順次割当データz、順次割当データzが割当てられた順次集約木を一意に特定できる順次集約木番号、順次割当データzが割当てられた順次集約木のリーフを一意に特定できる順次集約木リーフ番号、およびその時点で取得できる順次集約補完データの一部（これを登録点の即時補完データと言う） SKの位置情報及び割当値を含むように構成されている。

【００８９】
また、同図によれば、証明応答には、利用者装置21の直前の登録点の遅延補完データTK2の位置情報及び割当値も含むように構成されている。

【００９０】
ここで、本実施の形態における証明応答の具体例を図4を用いて説明する。尚、上述したように、この証明応答の形式を「連鎖補完方式」と呼ぶ。今、ある利用者装置51からの登録点がX1（ノード(0，2)），X2（ノード(0，11)），X3（ノード (0，18)），X4 （ノード(0，21)），X5 （ノード(0，29)），X6（ノード (0，31)）であるとする。

【００９１】
連鎖補完方式においては各登録点において以下のようなデータが利用者装置51に返されるようになっている。

【００９２】
（１）X1点における証明応答には、X1点の即時補完データが返される（具体的には、ノード(1，0)の割当値）。

【００９３】
（２）X2点における証明応答には、X2点の即時補完データ、及びX1点のX2点における遅延補完データが返される（具体的には、X2点の即時補完データとして、ノード(3，0)，ノード(1，4)，ノード(0，10) の割当値、X1点のX2点における遅延補完データとして、ノード(0，3)，ノード(2，1) の割当値）。

【００９４】
（３）X3点における証明応答には、X3点の即時補完データ、及びX2点のX3点における遅延補完データが返される（具体的には、X3点の即時補完データとして、ノード(4，0)，ノード(1，8) の割当値、 X2点のX3点における遅延補完データとして、ノード(2，3) の割当値）。

【００９５】
（４）X4点における証明応答には、X4点の即時補完データ、及びX3点のX4点における遅延補完データが返される（具体的には、X4点の即時補完データとして、ノード(4，0)，ノード(2，4)，ノード(0，20) の割当値、 X3点のX4点における遅延補完データとして、ノード(0，19) の割当値）。

【００９６】
以下、X5及び X6 においても同様である。このように、連鎖補完方式においては、証明応答として、ある登録点に関して、該登録点の即時補完データ及び該登録点の直前登録点

の該登録点における遅延補完データが含まれるようになっている。これにより、連鎖補完方式においては、過去の登録点が増えても証明要求に対する証明応答のデータ量が比例的に増加しないので、証明装置4と利用者装置5i間の通信データ量を抑制することができる。尚、各証明応答は、利用者装置2iごとに管理されるようになっている。

【００９７】

次に、連鎖補完方式の証明応答であっても、利用者装置5iは、実質的には、シーケンス補完方式の証明応答と同一のデータが得られることを図11及び図１２を参照して説明する。

【００９８】

図11に示すように、順次集約木 ST2 の３つのリーフa1, a2, a3 が左からこの順番であるものとすると、 a2点のa3点における遅延補完データ、a2点の即時補完データ、及びa1点のa2点における遅延補完データから、a1のa3点における遅延補完データは、以下のように計算される。

【００９９】

まず、a2点のa3点における遅延補完データの中で最もレベルが高いノードのレベルをj2と置く。また、a1のa2による認証点をAP(a1, a2)、 その兄弟ノードをAP'(a1, a2) と書き、 AP(a1, a2) のレベルをj1と置く。

【０１００】

このとき、第１に、a1点のa3点における遅延補完データに含まれる認証パスノードのうちレベルがj1よりも小さいものの割当値は、a1点のa2点における遅延補完データに含まれる。

【０１０１】

また、第２に、a1点のa3点における遅延補完データに含まれる認証パスノードのうちレベルがj1に等しいものの割当値は、a2点のa3点における遅延補完データおよびa2点の即時補完データから計算できる。

【０１０２】

さらに、第３に、a1点のa3点における遅延補完データに含まれる認証パスノードのうちレベルがj1により大きいものの集合は、a2点のa3点における遅延補完データに含まれる認証パスノードのうちレベルがj1より大きいものの集合と等しい。従って、a1点のa3点における遅延補完データに含まれる認証パスノードのうちレベルがj1より大きいものの割当値は、a2点のa3点における遅延補完データから計算できる。

【０１０３】

以上から、a1点のa3点における遅延補完データは、以下の３つのデータから計算することができる。

【０１０４】

(1) a2点のa3点における遅延補完データ
(2) a2点の即時補完データ
(3) a1点のa2点における遅延補完データ

尚、上記の(1), (2), (3) からa1点のa3点における遅延補完データを計算する処理を完全化波及処理と呼ぶ。

【０１０５】

この完全化波及処理を用いることにより、利用者装置5iは、連鎖補完方式の証明応答からシーケンス補完方式の証明応答を計算することができるようになっている。図12 はこの計算方法を示す表である。ここで、図12は、シーケンス補完方式及び連鎖補完方式において、各登録点に必要な即時補完データ及び遅延補完データを示している。尚、連鎖補完方式における証明応答の即時補完データ及び遅延補完データは、２重線に囲まれる部分のデータである。また、図12に示す矢印は計算の方向を示している。例えば、図12によれば、a2のa3における遅延補完データ（P1）、a2の即時補完データ（P2）、及びa1のa2における遅延補完データ（P3）から、a1のa3における遅延補完データ（P4）が計算できることを示している。|

同様にして、a3のa4における遅延補完データ（P5）、a3の即時補完データ（P6）、及びa2のa3における遅延補完データ（P1）から、a2のa4における遅延補完データ（P7）が計算できる。そして、これを繰り返すことにより、連鎖補完方式であっても、最終的には、図12に示す遅延補完データすべてが計算できることになる、これは、シーケンス補完方式の証明応答に他ならない遅延補完データである。

【０１０６】

従って、本実施の形態の連鎖補完方式であっても、利用者装置5iにおいては、図12に示すような完全化波及処理を行うことにより、第１の実施の形態と同様の検証をすることができるものである。尚、この完全化波及処理に関しては、後述する「インクリメンタル完全化」の処理として、詳しく説明する。

【０１０７】

利用者装置51は、コンピュータネットワーク3を介して証明装置4とデータを送受信する送受信部21、所定のデジタル・データを含む証明要求を複数回行うイベント順序証明要求証部22、証明要求に対する証明応答に含まれた受理証明書を検証するイベント順序証明検証部51、受理証明書を含む証明応答をはじめとしてイベント順序証明に関する情報を記憶する記憶部52を有する構成である。

【０１０８】

ここで、イベント順序証明検証部51は、第１の実施の形態のイベント順序証明検証部23の機能に加えて、後述するインクリメンタル完全化の処理を行う機能を具備するもので、受理証明書に対して以下の検証機能を備える。

【０１０９】

第１の検証機能としては、証明装置4のデジタル署名作成部14及び電子的情報公表部15を介して公表される公表情報に、受理証明書に含まれる順次割当データがハッシュ関数を介してリンクすることを検証するものである。具体的には、順次集約木のルート値が公表された値と利用者装置51で計算されたルート値が一致するか否か検証するものである。

【０１１０】

第２の検証機能としては、公表情報が公開される前であっても、利用者装置51間における受理証明書発行の時間的前後を検証するものである。

【０１１１】

以下、第２の検証機能を図5を用いて説明する。

【０１１２】

今、２つの利用者装置2A及び2Bが、それぞれ、連鎖補完方式により、各登録点の証明応答を取得するものとし、図５に示すa，a_1，a_2，a_fを利用者装置2Aの登録点、bを利用者装置2Bの登録点とする。尚、a_fは、暫定終端点である。図５においては、利用者装置2Aの１つの登録点a があり、それより右に位置する利用者装置2Bの登録点bがあり、さらにその右に位置する利用者装置2Aの登録点a_f がある。

【０１１３】

本実施の形態においては、まず、利用者装置2Aの登録点a に対して、a_f を暫定終端点として、図12に示す完全化波及処理を行う。これにより、シーケンス補完方式と同一の証明応答が得られるので、その後は、第１の実施の形態のときと同一の方法を実施することにより、登録点aと登録点bの時間的前後を検証することができる。即ち、本実施の形態においても、登録点a_fを現時点としたときの現時点順次集約木における、登録点a の 登録点bによる認証点oの割当値V(o)が一致すれば、登録点ａの登録が登録点ｂの登録より前に起こったことを客観的に証明することができる。

【０１１４】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（CPU：Central Processing Unit）、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置（メモリ）、ハードディスク（HD）等の電源断時にもデータを記憶し続けることができる２次記憶装置を有する電子的な装置から構成されている。このうち、証明装置4のイベント順序証明応答作成部41及び利用者装置51のイベント

順序証明検証部51の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、証明装置4の記憶部42及び利用者装置51の記憶部52は、上記主記憶装置あるいは２次記憶装置の機能を備えたものである。

【０１１５】

（２－２．システム動作）

ここで、以上の構成を有するイベント順序証明システム200におけるイベント順序証明方法に関しては、図６における証明装置1及び利用者装置21を、それぞれ証明装置4及び利用者装置51に置き換えたものと同一であるため、説明を省略する。また、イベント順序証明検証方法に関しては、図7及び図8における利用者装置2A及び2Bを、それぞれ利用者装置5A及び5Bに置き換えたものであるとともに、事前ステップとして、利用者装置5A及び5Bそれぞれにおいて、後述するインクリメンタル完全化処理を実行すれば、その後の動作は、図7及び図8の動作と同一であるため、説明を省略する。

【０１１６】

＜２－３．証明装置4のデータ記憶方法＞

（第１の方法）

次に、連鎖補完方式における証明装置4のデータ記憶方法について、より詳細に説明する。まず、第１の方法は、証明装置4が順次集約木を記憶部42上に構成することにより、上述の連鎖補完の方式を実現する方法（以下、方法Ａという.）である。

【０１１７】

図13は、方法Ａを採用したときの記憶部42に記憶されるデータの概略構成を示す図である。図13に示すように、記憶部42には、順次集約木そのもの、即ち、証明要求が割り当てられたノード、計算可能なノードの位置情報及び割当値を記憶するとともに、各利用者装置51ごとに直前登録点の位置情報を記憶するようになっている。

【０１１８】

この方法Ａにおいては、証明要求を証明装置4が受信するたびに、記憶部42上に記憶する順次集約木に、レベルが0のノード、即ちリーフを加え、レベルが１以上のノードで割当値が計算できるものに対しては、そのノードを順次集約木に追加しその割当値を付加して、記憶部42上に順次集約木を構築するようになっている。

【０１１９】

以下に、方式Ａにおける証明装置4の動作を図14を用いて説明する。ここで、図14は、証明装置4のイベント順序証明要求集約部12及びイベント順序証明応答作成部41の機能を示すフローチャート図である。

【０１２０】

まず、証明装置4は利用者装置51から証明要求を受けると、証明要求から順次割当データを生成し、順次集約木の新しいリーフに割り当てて、新登録点とするとともに、該登録点のノード情報（位置情報及び割当値）を記憶する（ステップS1101，S1103）。

【０１２１】

次いで、新登録点の即時補完データを即時補完データの定義に従って、記憶部42に記憶された順次集約木から取得する（ステップS1105）。

【０１２２】

次いで、新登録点の追加により、レベルが１以上のノードで割当値が計算できるものに対しては、割当値を計算して、そのノードの位置情報及び割当値を記憶部41に記憶する（ステップS1107）。

【０１２３】

次いで、直前登録点の遅延補完データを、遅延補完データの定義に従って、記憶部41に記憶された利用者装置51ごとの直前登録点及び順次集約木から取得する（ステップS1109）。

【０１２４】

次いで、新登録点を直前登録点とし、該利用者装置51の直前登録点として記憶するとともに、ステップS1105及びS1109で取得した即時補完データ及び遅延補完データを含む証明

応答を作成し、利用者装置51に送信する（ステップS1111，S1113，S1115）。

【０１２５】

（第２の方法）

次に、第２の方法は、証明装置4が順次集約木を記憶部42上に構成するのではなく、スタック構造を記憶部42に構成することにより、上述の連鎖補完の方式を実現する方法（以下、方法Ｂという）である。方法Ｂは、順次集約木の大きさにほぼ比例して必要記憶量が増加する方法Ａをさらに改善したものであり、スタック構造を用いて順次集約木のノード割当値、各順序証明要求に対する即時補完データ、及び遅延補完データを計算するので、必要記憶量を減少することができ、証明装置4の記憶部42に収まらない大きさの順次集約木の取り扱いを可能とすることができる。

【０１２６】

図15は、方法Ｂを採用したときの記憶部42に記憶されるデータの概略構成を示す図である。図15に示すように、記憶部42には、即時補完データ（位置情報及び割当値）を記憶する第１のスタック421と利用者装置51ごとに遅延補完データを記憶する記憶部422を備えており、利用者装置51ごとに遅延補完データを記憶する記憶部422は、直前登録点（位置情報）423及び遅延補完データ（位置情報及び割当値）を記憶する第２のスタック424で構成されている。尚、第１又は第２のスタックの要素となるようなデータをスタックフレームと呼ぶ。

【０１２７】

ここで、上記2種類のスタックのうち第１のスタックは、従来から用いられているデータ構造である。例えば、R. Merkle: Secrecy, Authentication, and Public Key Systems, UMI Research Press, 1982. の36ページには二分木のルートノードの割当て値を計算するための再帰的手順 H(a, b)が記載されているが、この再帰的手順を１つのスタックを用いて標準的に実装するとき、このスタックは上記第１のスタックと同様の使われ方をする。

【０１２８】

以下に、方式Ｂにおける証明装置4の動作を図16を用いて説明する。ここで、図16は、証明装置4のイベント順序証明要求集約部12及びイベント順序証明応答作成部41の機能を示すフローチャート図である。

【０１２９】

まず、証明装置4は利用者装置51から証明要求を受けると、証明要求から順次割当データを生成し、順次集約木の新しいリーフに割り当てて、新登録点とする（ステップS1121，S1123）。

【０１３０】

次いで、新登録点の即時補完データを第１のスタック421から取得する（ステップS1125）。

【０１３１】

次いで、新登録点の位置情報及び割当値を含むスタックフレームを第１のスタックに追加する（ステップS1127）。その際、新たに第１のスタックに追加されたスタックフレームが、他の利用者装置51において、直前登録点の補完データに対応するものであるときは、該スタックフレームを該当する利用者装置51の第２のスタックに追加する（ステップS1129，S1131）。

【０１３２】

次いで、第１のスタックに兄弟ノードである２つのノードに対応する２つのスタックフレームが存在する限り、当該の２つのノードの親に当たるノードの位置情報と割当値を含むスタックフレームを生成し、当該の２つのノードに対応するスタックフレームを第１スタックから除き、上記新たに生成したスタックフレームを第１スタックに追加する（ステップS1133，S1135，S1137，S1139）。その際、新たに第１のスタックに追加されたスタックフレームが、他の利用者装置51において、直前登録点の補完データに対応するものであるときは、該スタックフレームを該当する利用者装置51の第２のスタックに追加する（ス

テップS1141,S1143）。

【０１３３】

次いで、当該の利用者装置51に対する第２のスタックから直前登録点の新登録点における遅延補完データを取得し，当該の利用者装置51に対する第２のスタックを空にする（ステップS1145）。

【０１３４】

次いで、新登録点を直前登録点とし、該利用者装置51の直前登録点として記憶するとともに、ステップS1125及びS1145で取得した即時補完データ及び遅延補完データを含む証明応答を作成し、利用者装置51に送信する（ステップS1147，S1149,S1151）。

【０１３５】

上記動作を図4に示す具体例を用いて説明する。尚、新登録点をX4として説明する。

【０１３６】

まず、証明装置4は利用者装置51から証明要求を受けると、証明要求から順次割当データを生成し、順次集約木の新しいリーフである登録点X4に割り当てて、新登録点とする（ステップS1121,S1123）。

【０１３７】

次いで、新登録点X4の即時補完データであるノード(3,0)の割当値を第１のスタック421のスタックフレーム0から、ノード(2,4)の割当値を第１のスタック421のスタックフレーム1から、ノード(0,20)の割当値を第１のスタック421のスタックフレーム2からそれぞれ取得する（ステップS1125）。

【０１３８】

次いで、新登録点（0,21）の位置情報及び割当値を含むスタックフレーム3を第１のスタックに追加する（ステップS1127）。その際、新たに第１のスタックに追加されたスタックフレームが、他の利用者装置51において、直前登録点の補完データに対応するものであるときは、該スタックフレームを該当する利用者装置51の第２のスタックに追加する（ステップS1129,S1131）。

【０１３９】

次いで、第１のスタックに兄弟ノードに対応する２つのスタックフレームが存在するので（スタックフレーム2及び3）、当該の２つのノードの親に当たるノード（1,10）の位置情報と割当値を含むスタックフレームを新たに生成し、当該兄弟ノードに対応するスタックフレーム（スタックフレーム2及び3）を第１スタックから除き、上記新たに生成したスタックフレームを新たなスタックフレーム2として第１スタックに追加する（ステップS1133,S1135，S1137，S1139）。その際、新たに第１のスタックに追加されたスタックフレームが、他の利用者装置51において、直前登録点の補完データに対応するものであるときは、該スタックフレームを該当する利用者装置51の第２のスタックに追加する（ステップS1141,S1143）。

【０１４０】

次いで、当該の利用者装置51に対する第２のスタックから直前登録点X3の新登録点X4における遅延補完データであるノード(0,19)の割当値を第２のスタック424のスタックフレーム0から取得し，当該の利用者装置51に対する第２のスタックを空にする（ステップS1145）。

【０１４１】

次いで、新登録点X4を直前登録点X3とし、該利用者装置51の直前登録点423として記憶するとともに、ステップS1125及びS1145で取得した即時補完データ及び遅延補完データを含む証明応答を作成し、利用者装置51に送信する（ステップS1147,S1149,S1151）。

【０１４２】

（第２の方法の実装例）

以下に、上述した方法Ｂを用いた証明装置4の証明応答作成の一実装例を説明する。

【０１４３】

図17は証明装置4の記憶部42の構成を示す図である。図17に示すように、順次集約木の

ノード割当値を計算するノード割当値計算用スタック（以下では-stackと呼ぶ）及び遅延補完用データ構造の配列（以下では-chain-comple-data-vec と呼ぶ）を持つ。-stackの要素はスタックフレームからなるスタック構造であり、各スタックフレームはplace部とvalue部からなる。このうちplace部は順次集約木のノード位置を表すプレースを保持し、そのノードのレベルを示すlevel部とレベル内の番号を示すindex部の組からなる。value部はそのノードの割当値を保持する。-chain-comple-data-vec はデータ構造chain-comple-dataの配列であり、データ構造chain-comple-data は late-ccomple-stack部、prev-point部、prev-point-old部、及び old-tree-id部からなる。このうち、late-ccomple-stack部は-stackと同様にスタックフレームからなるスタック構造であり、prev-point部は直前の登録点を表す識別番号（非負整数またはnil）を表し、prev-point-old部は現在の集約木より前に生成された集約木における直前の登録点を表す識別番号（非負整数またはnil）を表し、old-tree-id部はprev-point-old部がnilではないときprev-point-old部が示す登録点が属する集約木の識別番号（非負整数または nil ）である。

【０１４４】

図18は、証明装置4における連鎖補完の手順 GET-REQを示す。この手順で使用される変数及び関数は以下のとおりである。

【０１４５】

・v0 はデジタル・データ（通常はハッシュ値）を保持する変数である。

【０１４６】

・idx0 は利用者識別番号を表す整数を保持する変数である。

【０１４７】

・-lev0-ptr は次に受付けたイベント順序証明要求を割当てるリーフの識別番号を保持する変数であり、初期値は0である。

【０１４８】

・place0 は順次集約木のノード位置を表すプレースを保持する変数である。

【０１４９】

・sflm0 はスタックフレームを保持する変数である。

【０１５０】

・F(v0) はイベント順序証明要求に含まれるデジタル・データv0 を順次集約木リーフに割当てるデータに変換する関数を表す。F(v0) は v0 と等しいとすることにしてもよいし、あるいはv0 に所定のハッシュ関数（例えば SHA1）を適用した結果とすることにしてもよい。

【０１５１】

・-tree-id は順次集約木の識別番号を保持する変数である。

【０１５２】

・make-stackflm(place0, V0) はプレース placeとデジタル・データ V0を引数とし、place0をplace部として持ち、V0をvalue部としてもつスタックフレームを返す関数である。

【０１５３】

・stack-bufはある瞬間のスタックの状態を保持する変数である。

【０１５４】

・handle-chain-comple(id0、 tree-id0, idx0, V0,
prev-point0, immed-stack-data0, late-stack-data0)

は、順次集約木の識別子 tree-id0、リーフの識別子 idx0、 割当てデータ V0、 即時補完データ immed-stack-data0、遅延補完データ late-stack-data0 から構成される受理証明書を作成し、利用者識別番号 id0を持つ利用者装置5iに向けて送付する関数を表す。

【０１５５】

証明装置4が証明要求を受信する度に、要求者から受付けたデジタル・データをv0、要求者の識別番号を id0 としてこの手順が呼び出される（ステップST101 ～ST117）。

【0.１５６】

図19は、図18の手順 GET-REQから呼び出される、ノード値計算処理の手順 COMP-NODE-

VALS を表す。この手順で使用される変数及び関数は以下のとおりである。

【０１５７】

・sflmlb はスタックフレームを保持する変数である。

【０１５８】

・placelb はプレースを保持する変数である。

【０１５９】

・idxlbは整数を保持する変数である。

【０１６０】

・levlbは整数を保持する変数である。

【０１６１】

・vallb はデジタル・データ（通常はハッシュ値）を保持する変数である。

【０１６２】

・sflm0b はスタックフレームを保持する変数である。

【０１６３】

・place0b はプレースを保持する変数である。

【０１６４】

・lev0b は整数を保持する変数である。

【０１６５】

・lev-nw 及び idx-nw は 整数を保持する変数である。

【０１６６】

・floor(x) は実数xを引数として、x を超えない最大の整数を返す関数である。さらにy ≠0 に対して、floor(x, y) = floor(x／y) と書く。即ち、floor(x, y) はx をy で割った際の整商である。

【０１６７】

・hash-comb2(val0, vall) はビット列で表される２つのデジタル・データval0 とvall を引数とし、val0 と vall を連接し、所定のハッシュ関数(SHA1等）を適用した結果を返す関数とする。

【０１６８】

図20は、図18の手順 GET-REQ及び図19の手順COMP-NODE-VALSから呼び出される、遅延データ設定処理の手順 REGISTER-COMPLE-DATA を表す。この手順で使用される変数及び関数は以下のとおりである。

【０１６９】

・place はプレースを保持する変数であり、sflm はスタック・フレームを保持する変数である。

【０１７０】

・id は利用者識別番号を表す整数を保持する変数である。

【０１７１】

・N は登録された利用者の総数を保持する変数である。

【０１７２】

・auth-node-pl(prev-point, place) は 順次リーフの識別番号である prev-point とプレース place を引数とし、place の割当値が prev-point の遅延補完データに含めるべきものであれば true をさもなければ false を返す関数である。place = (j, i) としたとき、auth-node-pl(prev-point, place) がtrue となるための 必要十分条件は、floor(prev-point, 2^j) が偶数で、i = floor(prev-point, 2^j) ＋ 1 となることである。

【０１７３】

次に、図21及至図23を参照しながら、１つ集約間隔が終わり、該集約間隔に対する順次集約木を終端し、次の集約間隔に対する次の順次集約木を初期化する順次集約木切替処理について説明する。

【０１７４】

図21は順次集約木切替処理のメインルーチンを表す。このルーチンにおいては、図22で

記述されたサブルーチンTERMINATE-STREE-SUB1 と図23で記述されたサブルーチンTERMINATE-STREE-SUB2 を実行後、大域変数 -tree-id を1だけインクリメントし、2つの大域変数 -lev0-ptr と -stack を初期化した後終了する。これらの大域変数は図18で記述した手順 GET-REQ で用いたものである。

【0175】

図22で記述するTERMINATE-STREE-SUB1は、その集約間隔が終了する時点で構成されている順次集約木を基に必要に応じてノードを追加し、それらのノードには前以て定めた手順に従って所定のハッシュ値を割当、当該の集約木のルート値を定義する処理を記述している。

【0176】

図24を参照しながら、TERMINATE-STREE-SUB1の動作を、特定の状況に則して具体的に説明する。リーフ識別番号9 の処理が終了後、リーフ識別番号10の処理に入る前に集約間隔が終了し、TERMINATE-STREE-SUB1を呼び出す状況を考える。開始の時点では -stack の状態は、トップから見て [(1, 4), V(1, 4)] と [(3, 0), V(3, 0)]を含むものとなっている。手順 TERMINATE-STREE-SUB1 により、ノード (1,5) と (2, 3) にダミーのハッシュ値を割当て、この順次集約木のルート値を定め、同時に各登録点の完全認証パスデータ（ルート値が計算できる認証パスノードの集まり）を定義することが、以下の(1)～(4)に示すようにできる。

【0177】

(1) ステップST1211 により、局所変数 sfml-xb に [(1,4), V(1, 4)] が設定され、-stack は[(3, 0), V(3, 0)]のみを含むものとなる。次にステップST1212により局所変数 place-xbに (1, 4)が、idx-xbに4 が設定される。

【0178】

ステップST1213では idx-xbが偶数か否かの判定をするが、現在のidx-xb の値 4 は偶数であるので、ステップST1214 に進む。

【0179】

ステップST1214では -stack が nil であるか否か判定するが、-stack は nil ではないのでステップST1215に進む。

【0180】

ステップST1215では、局所変数 lev-xb に1を設定し、val-xb に V(1, 4) を設定し、idx-1b に1＋4 ＝5を設定する。さらに、place-1b に (lev-xb, idx-1b) ＝ (1, 5) を設定。この位置情報 (1, 5) が最初のダミー・ノードを表す。この最初のダミー・ノードに割当てるハッシュ値を計算する関数 dummy-hashを呼びだし、その返り値を dum-val-1b に設定する。さらにsfml-1b に

make-stackflm(place-1b, dum-val-1b) ＝[(1, 5), dum-val-1b]

を設定する。ここでmake-stackflmはノードの位置情報とハッシュ値を引数としてスタックフレームを生成する関数である。ここでplac-1b と sfml-1b を引数として REGISTER-COMPLE-DATA （図20で定義したもの）を呼び出す。

【0181】

続いて、ステップST1216において、lev-nw に2を設定し、idx-nw に floor(idx-xb, 2) ＝ floor(4, 2) ＝2 を設定し、さらにplace-nw に(2, 2) を設定する。続いて、val-nw にhash-comb2(val-xb, dum-val-1b) を設定する。hash-comb2 は2つのハッシュ値を引数として、それらを連接し、所定のハッシュ関数を適用した結果を返す関数である。 sfml-nw にmake-stackflm(place-nw, val-nw)を設定し、sfml-nw を -stack にプッシュする。これにより、-stack は[(2, 2), V(2,2)], [(3, 0), V(3, 0)] を含む構成となる。更にplace-nw とsfml-nw を引数としてREGISTER-COMPLE-DATA を呼び出す。ここでステップST1211に戻る。

【0182】

(2) ステップST1211において -stack を1つポップし、sflm-xb に [(2, 2), V(2, 2)] を設定する。（ここで-stackの状態は、[(3, 0), V(3, 0)] となる。）更にplace-xb に

(2, 2) を、idx-xb に2 を設定する。

【０１８３】

ステップST1213 において idx-xbの値2は偶数と判定されステップST1214に進み、-stackはnilではないので、さらにステップST1215に進む。lev-xb に2を設定し、val-xb に V(2, 2) を設定し、idx-1b に3 を設定し、place-1b に (2, 3) を設定し、dum-val-1bに dummy-hashの返し値を設定し、この値をV(2, 3)と表す。さらにsfml-1b に

make-stackflm(place-1b, dum-val-1b) ＝[(2, 3), V(2, 3)]

を設定する。ここでplace-1b と sfml-1b を引数として REGISTER-COMPLE-DATA を呼び出す。

【０１８４】

続いて、ステップST1216において、lev-nw に3を設定し、idx-nw に floor(val-xb, 2) ＝ floor(2, 2) ＝1 を設定し、さらにplace-nw に(3, 1) を設定する。続いて、val-nw にhash-comb2(val-xb, dum-val-1b) を設定し、この値をV(3, 1)と書く。 sfml-nw にmake-stackflm((3, 1) , V(3, 1))を設定し、sfml-nw を -stack にプッシュする。これにより、-stack は[(3, 1) , V(3,1)] , [(3, 0), V(3, 0)] を含む構成となる。さらにplace-nw とsfml-nw を引数としてREGISTER-COMPLE-DATA を呼び出す。ここでステップST1211に戻る。

【０１８５】

(3)ステップST1211 において -stack を１つポップし、sflm-xb に [(3, 1), V(3, 1)] を設定する。（-stackの状態は、[(3, 0), V(3, 0)] となっている。）さらに、place-xb に (3, 1) を設定し、idx-xb に1 を設定する。

【０１８６】

ST1213 において idx-xbの値1は奇数と判定され、ST1217に進み、lev-xb に3を設定し、val-xb にV(3, 1) を設定する。-stack をポップしポップされた [(3, 0), V(3, 0)] をsfml0bに設定する。さらに、place-0b に(3, 0) を、lev-0b に 3 を、idx-0b に0を、val-0b にV(3, 0) を設定する。

【０１８７】

ステップST1218 において、lev-nw に4 を設定し、indx-nw に floor(1, 2) = 0 を設定し、place-nw に (4, 0)を設定し、val-nw に hash-comb2(V(3,0),V(3, 1)) を設定する。この値をV(4, 0)とする。 sfml-nw にmake-stackflm((4, 0),V(4, 0))を設定し、sfml-nw を -stack にプッシュする。これにより、-stack は[(4,0), V(4, 0)]を含む構成となる。 さらに place-nw とsfml-nw を引数としてREGISTER-COMPLE-DATA を呼び出す。ここでステップST1211に戻る。

【０１８８】

(4)ステップST1211において、-stack を１つポップし、sflm-xb に [(4, 0), V(4, 0)] を設定する。（-stackの状態は nil となっている。）さらに、place-xb に (4, 0) を設定し、idx-xb に0 を設定する。ステップST1213 においてidx-xbの値0は偶数と判断され、ステップST1214に進み -stack はnilであるので、ステップST1219に進み、返し値に V(4, 0) を設定して終了する。

以上の結果、この手順の返し値は 当該の順次集約木のルート値である V(4,0)となる。

【０１８９】

次に、図23で記述されたサブルーチンTERMINATE-STREE-SUB2について説明する。

【０１９０】

まず以下の変数および定数が使用される。

【０１９１】

・ 利用者装置の識別子である非負整数を保持する変数 id
・ 利用者装置の総数を表す定数 N
・ 図17の遅延補完用スタックの 配列 -chain-comple-data-vec の各要素と同じ構造を持つchain-comple-data2
・非負整数またはnilを保持する変数prev-chain-point2。

【０１９２】
次にTERMINATE-STREE-SUB2の動作について説明する。
【０１９３】
id ＝0，…，N－1 について図23のブロック1 を実行する。
【０１９４】
ブロック１の中では以下の動作をする。
【０１９５】
chain-comple-data2 に -chain-comple-data-vec[id] を設定し、prev-chain-point2 にchain-comple-data2のprev-point部を設定する （ステップST1222）。
【０１９６】
prev-chain-point2がnil であればブロックを終了する（ステップST1223）。
【０１９７】
さもなければ、chain-comple-data2 のprev-point-old部をprev-chain-point2 に、prev-point部をnil に、old-tree部に現在の集約木識別子を各々設定し、次に-chain-comple-data-vec[id] にchain-comple-data2 を設定する（ステップST1224）。
【０１９８】
＜２－４．利用者装置5|におけるインクリメンタル完全化＞
次に、利用者装置5|におけるインクリメンタル完全化の処理について、詳しく説明する。ここで、インクリメンタル完全化には、大別して（１）インクリメンタル個別完全化と（２）インクリメンタル一括完全化の２つの処理があり、いずれかが利用者装置5|において実行されるものである。尚、上述した「完全化波及処理」は、インクリメンタル一括完全化の中の一機能を説明したものである。
【０１９９】
（インクリメンタル個別完全化）
利用者装置2Aのある集約間隔|に属するか或いは或いはその次の集約間隔の最初の登録点であるよう登録点$a_{|}$を暫定終端点とする。
【０２００】
$a_{|}$ がある集約間隔|の次の集約間隔の最初の登録点であるとき、当該の集約間隔|に対する追伸点と呼ぶ。
【０２０１】
集約間隔|の間に、この暫定終端点$a_{|}$までに登録した登録点の集合を
a(0)，a(1)，…，a(n) とする。
【０２０２】
（通常は、a(n)＝$a_{|}$であるが、$a_{|}$ が追伸点であるときはこうはならない。）
このとき、登録点の集合から、$a_{|}$を暫定終端点としたときの１つあるいは複数の順次集約小木が構成され、構成された順次集約小木の集まりを、$a_{|}$を暫定終端点としたときの順次集約フォレストと呼ぶことにする。
【０２０３】
図25を参照して、順次集約フォレストと順次集約小木について具体的に説明する。
【０２０４】
$a_{|}$ が当該の集約間隔にあるとき、$a_{|}$ がリーフ番号（非負整数）を表し、$a_{|}$ の二進表現においてはk(1)，k(2)，…，k(m) 桁において１が立つものとする（但し最小桁は0桁とする）。図25においては、m ＝ 4 としている。ここで、k(m) は0でもよく、k(1)＞k(2)＞ k(3) ＞ … ＞k(m) とならなければならない。このとき、上記順次集約フォレストに属するn番目の順次集約小木のリーフの数は $2^{k(n)}$ となる。図25においては、ST2(1)，…，ST2(4) が順次集約小木を表している。
【０２０５】
インクリメンタル個別完全化とは、指定されたa ∈{a(0)，a(1)，…，a(n)} について、以下の計算(1)、(2)、(3) を行うことである。
【０２０６】

(1) a が属する順次集約小木ST（ユニークに定まる）を計算する。

【０２０７】

(2) 順次集約フォレストにおいて上記STより左に位置する１つあるいは複数の順次集約小木のルートの割当値を、a(0)，…，a(n)（及び a_f ）で取得する補完データから計算する。

【０２０８】

(3) ST におけるa の認証パスを $authPath_{ST}(a)$ とおくと、$authPath_{ST}(a)$ に属するノードの割当値を、a(0)，…，a(n)（及び a_f ）で取得する補完データから計算する。

【０２０９】

尚、インクリメンタル個別完全化の定義は、以下に定義する現時点順次集約木を用いて行うこともできる。ここで、現時点順次集約木とは、a_fを暫定終端点としたときの順次集約フォレストを含むような最小の二分木を、a_fを暫定終端点としたときの現時点順次集約木という。

【０２１０】

図26は、現時点順次集約木の枝を実線及び点線で示すものである。このうち、点線で示す枝が順次集約フォレストには含まれないが現時点順次集約木を構成するために追加した枝である。また黒で塗りつぶされた小円が順次集約フォレストに含まれるノードであり、塗りつぶしがない小円が現時点順次集約木を構成するために追加したノードである。現時点順次集約木をCSTと表し、CSTにおけるaの認証パスを $authPath_{CST}(a)$ とおく。このとき、インクリメンタル個別完全化とは、指定されたa ∈{a(0)，a(1)，…，a(n)} について、$authPath_{CST}(a)$ に属し、既に割当値が定まっているノードの割当値を、a(0)，…，a(n)（及び a_f ）で取得する補完データから計算することと同値である。

【０２１１】

尚、順次集約フォレストのリーフの数の総数をN としたとき、現時点順次集約木の高さ h はN ≦2^k となる最小の非負整数 k となる。

【０２１２】

上述したことを踏まえて、第２の検証機能を説明した図5に戻ると、登録点aに対して、a_fを暫定終端点としてインクリメンタル個別完全化を行うと、認証点oの割当値V(o)が計算できることになる。これにより、登録点a_fを現時点としたときの現時点順次集約木における、登録点a の 登録点bによる認証点oの計算された割当値V(o)が、登録点bで取得される即時補完データに含まれれば、登録点ａの登録が登録点ｂの登録より前に起こったことを客観的に証明することができる。

【０２１３】

次に、図27及び図28を参照しながら、インクリメンタル完全個別化の動作について説明する。図27は、インクリメンタル完全個別化の動作を示すフローチャート図である。

【０２１４】

まず、暫定終端点a_fより以前の登録点で集約間隔lに属する登録点aを１つ指示する（ステップS510）。図28に示す順次集約フォレストにおいては、インデックス18のリーフ（ノード(0，18)）をaとしている。

【０２１５】

次に、登録点aが属する順次集約小木STを計算する（ステップS520）。図28に示す順次集約フォレストにおいては、構成済み順次集約小木のうち左から2番目のST2(2)が STとなる。

【０２１６】

次に、登録点a の ST における各遅延認証パスノード sを計算する（ステップS530）。図28に示す順次集約フォレストにおいては、インデックス19のリーフ（ノード(0，19)）とレベル2のインデックス5のノード（（ノード(2，5)）が遅延認証パスノードとなる。

【０２１７】

次に、各遅延認証パスノード sの取得参照点をそれぞれ決定する（ステップS540）。ここで、取得参照点及び取得タイミング点について説明する。尚、以下では、ある登録点a

の即時補完データと、a の次の登録点a1で取得されるaの遅延補完データの合併を、登録点aの連鎖補完データとよぶ。

【０２１８】

登録点a0が与えられたとき、そのauthPath(a0) でレベルｊのノード(j, s(j)) の割当値V(j, s(j))を計算するために十分な情報を補完データから直接取得できるかあるいは該データを基に計算により取得できる要求登録点をV(j, s(j)) の取得参照点と呼ぶ。そして、上記の必要な補完データを受信する登録点を取得タイミング点と呼ぶ。

【０２１９】

例えば、図4に示す順次集約木において、登録点X3が与えられたとき、遅延補完データの１つであるノード（0,19）の取得参照点は、登録点X3（ノード（0,18））、取得タイミング点は、登録点X4（ノード（0,21））となる。また、登録点X3が与えられたとき、即時補完データの１つであるノード（4,0）の取得参照点及び取得タイミング点は、登録点X3（ノード（0,18））となる。一般に、即時補完データに関しては、取得参照点と取得タイミング点は一致する。

【０２２０】

次に、ステップS540で決定された取得参照点をもとに、各認証パスノードｓの割当値を計算する（ステップS550）。

【０２２１】

以上により、登録点ａにおけるインクリメンタル完全化の処理が終了し、この計算結果を用いて、登録点ａの割当値を含む入力に衝突困難ハッシュ関数を適用し、V(root(ST)) を計算することができる。尚、上述した計算が可能であるのは、s の割当値の取得参照点および取得タイミング点がともに、暫定登録点a_l以前であることによる。

【０２２２】

（インクリメンタル個別完全化の実装例）

以下に、上述したインクリメンタル個別完全化の一実装例を説明する。

【０２２３】

まず、順次集約小木STを決定する計算手順 FOREST-SSTを図29に示す。これは、図27のステップS520に相当するものである。

【０２２４】

この手順で使用される変数及び関数は以下のとおりである。

【０２２５】

・入力としては、リーフ識別子 a （非負整数）、暫定終端点の識別子 fin（非負整数）
・出力としては、a が属する順次集約小木の一番左のリーフ識別子start（非負整数）、a が属する順次集約小木の一番左のリーフ識別子last （非負整数）
・変数としては、非負整数を保持する変数 rest, ht, leaf-num
・使用される関数として、log2(x) は、log2(x) 以下の最大の整数、expt(x, y) は、 x の ｙ 乗

このアルゴリズムは、リーフ識別子a （非負整数）と暫定終端点の識別子 fin (非負整数)を入力とし、該暫定終端点の登録が終了した時点における順次集約フォレストに属する順次集約小木でaが属するものをSTとしたとき、STの一番左に位置するリーフの識別子start（非負整数）と一番右に位置するリーフの識別子last（非負整数）の組を出力するものである。当該の順次集約小木STのリーフの数は、last－start＋1 となり、当該の順次集約小木の高さは、$\log_2$(last－start＋1) となる。

【０２２６】

図28で示した具体例について、図29の手順を適用すると以下のようになる。リーフ識別子a を18とおき，暫定終端点の識別子 fin を26とおく。このとき、図29の手順に従って計算すると、start として16が返され、last として23が返される。この出力から、a が属する順次集約小木は、図28のST2(2)であることが分かる。

【０２２７】

次に、インクリメンタル完全化における認証パスノード割当値の取得参照点決定手順 D

ECIDE-GET-POINT-Aを図30に示す。この手順は、指定された要求登録点の指定されたレベルの認証パスノードの割当値が、 との要求登録点の即時補完データあるいは遅延補完データから得られるかを決定するものであり、図27のステップS540に相当するものである。

【０２２８】

図31は、手順DECIDE-GET-POINT-A において使われるデータ構造と変数の一部を表す。データ構造chaindata は leaf-index部、rgt-value部、immediate部、late部からなる構造である。M を一つの利用者装置51が一つの集約間隔に送出する順序証明要求の最大数とする。

【０２２９】

この手順で使用されるその他の変数及び関数は以下のとおりである。

【０２３０】

・変数chiandata-store は要素数が Mの配列 で、配列の各要素がデータ構造chaindataを保持するようなものである（図31参照）。

【０２３１】

・chaindata0 はデータ構造chaindata を保持する変数である。

【０２３２】

・a0 は 順次集約木のリーフ識別子を表す整数を保持する変数である。

【０２３３】

・順次集約木のノード (j, i) に対して、subTree(j, i) は (j, i) をルートとするような順次集約木の部分木を表す。

【０２３４】

・順次集約木の部分木 ST に対して、leafs(ST) はST のリーフの集合を表す。例えば、leafs(subTree(j, i)) は部分木subTree(j, i)のリーフの集合である。また、height(ST) はSTの高さを表す。

【０２３５】

次に、図30に示すインクリメンタル完全化の認証パスノード割当値の取得参照点決定手順（DECIDE-GET-POINT-A）のアルゴリズムの根拠を図32に示す図をもとに説明する。

【０２３６】

ここで、 a_f を暫定終端点とする構成済みフォレスト内の順次集約小木のうちa0 が属すものを ST とおく（ a0 ∈leafs(ST) ）。

【０２３７】

また、ST 内のa0 の認証パスを $authPath_{ST}(a0)$ とおき、

$$authPath_{ST}(a0) = [(0, s(0)), (1, s(1)), \cdots, (k-1, s(k-1))]$$

と置く。（但し、k は構成済みフォレスト内のa が属する順次集約小木STの高さである。即ち、k = height(ST)。）以下では、非負整数n, m に対して、[n…m] はn以上でm以下の整数の集合を表すものとする。

【０２３８】

各 j ∈[0… k −1] に対して、(j, s(j)) がとの登録点の補完データから計算できるかを決定するアルゴリズムを以下に示す。

【０２３９】

$rtPath_{ST}(a0)$を STにおけるa のルート・パスとおき、

$$rtPath_{ST}(a0) = [(0, r(0)), (1, r(1)), \cdots, (k-1, r(k-1)), (k, r(k))]$$

とする。r(0) = a0 、root(ST) ＝ (k, r(k)) である。j ∈[0…k −1] とする。

【０２４０】

(1) (j, r(j)) が (j+1, r(j+1)) のleft-child であるとき

s(j) = r(j) + 1 であり、(j, s(j)) は (j+1, r(j+1)) の right-child である。leafs(subTree(j, r(j))) に属する要求登録点の中で、最も右に位置する点を計算し、al と置く。

【０２４１】

(1-1) al ≠a_f のとき

a1 の次の要求登録点をa2 と置く（a1 ≠a_f ではないのでこのようなa2が在る。a2 ≦ a_f ）。

【０２４２】

(1-1-1) a2 ∈leafs(subTree(j, s(j))) のとき

leafs(subTree(j, s(j))) に属する要求登録点で最も右に位置するものをa3 と置く。

【０２４３】

(1-1-1-1) a3 = last(leafs(subTree(j, s(j)))であるとき（図32(a)を参照）

即時補完データimmedData(a3)は、subTree(j, s(j)) におけるa3の完全補完データ cmpltData(subTree(j, s(j)), a3)を含む。従って、

immedData(a3) ⊢ V(j, s(j))

(尚、X⊢ Yは，X からYが計算できることを表す。)

このとき、V(j, s(j)) の取得参照点および取得タイミング点は共にa3 としてよい。

【０２４４】

(1-1-1-2) a3 ≠ last(leafs(subTree(j, s(j)))であるとき

(1-1-1-2-1) a3 ≠a_f であるとき（図32(b)を参照）

a3 の次の要求登録点をa4 と置く。（a3 ≠a_f なので、このようなa4がある。a4 ≦ a_f 。a4 は追伸点である可能性もある。）

a3 のa4 による認証点のレベルをj' とすると、j' ≧ j+1

従って、順次集約木の性質により、V(j, s(j)) はa3 で取得する即時補完データと、a4 で取得する（a3に対する）遅延補完データ から計算できる。即ち、

immedData(a3) ∪ lateData(a3, a4) ⊢ V(j, s(j))

（尚、aをa3 のa4による認証点とすると、 immedData(a4) にはV(a)が入っているが、 これがV(j, s(j)) とは限らないことに注意する必要がある。）

このとき、V(j, s(j)) の取得参照点をa3 、取得タイミング点をa4 としてよい。a3 ≦a_f かつa4 ≦ a_f である。

【０２４５】

(1-1-1-2-2) a3 ＝a_fであるとき（図32（c）を参照）

このとき、a_f を暫定終端点とする構成済みフォレストにおいて (j, s(j)) を含む順次集約小木はない。

【０２４６】

よって，ST は (j, s(j)) を含むことは無い。従ってこのような場合はあり得ない。

【０２４７】

(1-1-2) a2∈leafs(subTree(j, s(j))) ではないとき（図32(d)を参照）

V(j, s(j)) ∈ lateData(a1, a2) である。

【０２４８】

V(j, s(j)) の取得参照点をa1 、V(j, s(j)) の取得タイミング点をa2 としてよい。

【０２４９】

a1 ≦ a_f かつa2 ≦ a_f

(1-2) a1＝a_f であるとき（図32(e)）。

【０２５０】

このとき、a_f を暫定終端点とする構成済みフォレスト内に (j, s(j)) を含む順次集約小木はない。

【０２５１】

よって、ST は (j, s(j)) を含むことは無い。従って、このような場合はあり得ない。

【０２５２】

(2) (j, r(j)) が (j+1, r(j+1)) のright-child であるとき（図32(f)）

r(j) = s(j) + 1 であり、(j, s(j)) は (j+1, r(j+1)) の left-child である。

【０２５３】

V(j, s(j)) ∈ immedData(a)

V(j, s(j)) の取得参照点および取得タイミング点を共にa0としてよい。a0≦ a_f

以上から、図30に示すインクリメンタル完全化の認証パスノード割当値の取得参照点決定手順（DECIDE-GET-POINT-A）は、すべての場合分けを考慮した手順となっているので、図30に示すアルゴリズムは正しいことがわかる。

【０２５４】

次に、要求登録点aが与えられたとき、そのauthPath(a) に含まれるレベルｊのノード(j, a(j)) の割り当て値V(j, a(j))を計算する手順 COMPLETION-SUB1を図33に示す(但し、0 ≦ｊ＜kで k は順次集約木の高さ)。これは、図27のステップS550を中心に説明するフローチャートである。

【０２５５】

この手順で使用される変数及び関数は以下のとおりである。

【０２５６】

・chaindata0及びchaindata1 はデータ構造chaindata を保持する変数である。

【０２５７】

・immedData1 及び lateData1 はデータ構造 stackfim の線形リストを保持する変数である。

【０２５８】

・chaindata-storeは当該の集約期間における、各登録点において証明応答として受信したデータを格納する配列である。配列の各要素は、図31で定義したchaindataの構造を持つ。この配列のi番目の要素は、当該の集約間隔におけるi番目の登録点の即時補完データと、その直後の登録点で取得したi番目の登録点の遅延補完データを含む。

【０２５９】

(1)本手順は２つの引数（入力）をもち、第１の引数を配列 chaindata-store の index を表す整数 i0 とし、第２の引数を順次集約木のレベルを表す整数 j とする（ステップST5501）。

【０２６０】

(2) 局所変数 chaindata0 に chaindata-store[i0] を設定し（ステップST5502）、局所変数 a0 を chaindata1 の leaf-index 部とし（ステップST5503）、変数a1 に authPath(a0) のレベル j のノードの index を設定する（ステップST5504）。

【０２６１】

(3) 図30に記述の認証パスノード割当値の取得参照点決定手順 DECIDE-POINT-Aにより V(j, a(j)) の取得参照点a2（要求登録点の１つで、その点で得られた連鎖補完データから、V(j, a(j)) が計算できるもの）を決定する（ステップST5505）。

【０２６２】

(4) 配列 chaindata-store を探索し、leaf-index部が a2 であるような配列要素の index となる整数 i1 を決定する（ステップST5506)。

【０２６３】

(5) 変数chaindata1 にchaindata-store[i1] を設定する(ステップST5507)。

【０２６４】

(6) 変数rgt-val1 に chaindata1 の rgt-val部を、変数immedData1 に chaindata1 の immediate部を，変数lateData1 にchaindata1 のlate部を、各々設定する（ステップST5508）。

(7) rgt-val1、 immedData1、あるいはlateData1 にplace部が(j, a1) となるスタックフレームが含まれるかどうか判定する（ST5509）。

【０２６５】

(7-1) 含まれれば、その値を返す（ステップST5510）。

【０２６６】

(7-2) 含まれないときは、immedData1とlateData1 から、ハッシュ関数を介して計算できるノードの割当値をレベル0からレベルｊまで順次計算する（ステップST5511）。

【０２６７】

(7-2-1) 上記で順次計算された割り当て値に V(j, a(j))が含まれるか否か判定する（ス

テップST5512）。

【０２６８】

(7-2-1-1) 含まれれば、その値を返す（ステップST5513）。

【０２６９】

(7-2-1-2) 含まれなければ、エラーとする（ステップST5514）。

【０２７０】

図34は、要求登録点aが与えられたとき、そのauthPath(a) に含まれるレベルj のノード(j, a(j)) の割り当て値V(j, a(j))のリスト

[V(0, a(0)), V(1, a(1)), …, V(k−1, a(k−1))]

を計算する手順 COMPLETION-SUB1を表す(但し、0 ≦j <kで k は順次集約木の高さ)

この手順で使用される変数及び関数は以下のとおりである。

【０２７１】

・k を順次集約木の高さとする。

【０２７２】

・auth-node-vals は長さkの配列で，各配列要素はハッシュ値を保持するものとする。

【０２７３】

まず、 図33のCOMPLETION-SUB 1 を各j (0≦j<k)に適用し、authPath(a) に属する各ノードの割当値を計算し、計算結果を auth-node-vals[j] に格納する（ステップST5523, ST5524）。

【０２７４】

次に、auth-node-vals を返り値とし、終了する（ステップST5525）。

【０２７５】

（インクリメンタル一括完全化）

上述したインクリメンタル完全化の方法は、完全化の対象となる受理証明書を指定し、その指定された受理証明書の個別完全化を行う方法である。次に述べるインクリメンタル完全化の方法は、ある利用者装置51が連続して取得した一連の受理証明書を一括して、上記のインクリメンタル個別完全化により計算されるものと同じデータを計算する方法である。この種類のインクリメンタル完全化をインクリメンタル一括完全化と呼ぶ。即ち、一連の登録点a(0), a(1), …, a(n)全てに対して上記のインクリメンタル個別完全化により計算されるものと同じデータを一括して計算することを、インクリメンタル一括完全化という。

【０２７６】

インクリメンタル一括完全化は、上述した完全化波及処理を用いた以下の手順により実行できる。

【０２７７】

(1) a(0), …, a(n) を、ある集約間隔Iに属する、ある利用者装置51による一連の登録点とする。

【０２７８】

(2) 利用者装置51によるa(n) の次の登録点を a_f とする。a_f は追伸点であってもよい。

【０２７９】

(3) 図35で記述した手順COMPLETION-BULK-BACKWARD1 により、各a = a(n), …, a(0) を、この順にインクリメンタル完全化を行う。

【０２８０】

この手順により、各登録点 a(n−i) (但しi=0, …, n) に対してa_f を暫定終端点とした場合のインクリメンタル個別完全化が実現されることが、以下のように数学的帰納法により示される（図36及び図37を参照）。以下では、簡単のためa(0), …, a(n) が共通の順次集約小木ST2に属し、a_f は ST2の各リーフよりも右に位置する場合を考える。尚、一般の場合も同様である。

【０２８１】

i=0, …, n について、手順COMPLETION-BULK-BACKWARD1により追加されたものを含むa

(n－i) の遅延補完データと、a(n－i)で受信した即時補完データの合併は、a(n－i) のST2における全ての認証パスノードの割当値を含んでいることを示せばよい。

【０２８２】

（１）帰納法のベース

i＝0のときを考える。このとき、a(n－i) ＝ a(n) である。手順COMPLETION-BULK-BACKWARD1により、a(n) に対してはa$_1$ の登録処理の終了時点におけるa(n)の遅延遅延補完データが追加される（図35のステップST5003）。ここで、a$_1$の登録処理の終了時点においては順次集約小木のルート値は確定しているので、手順COMPLETION-BULK-BACKWARD1により追加されたものを含むa(n) の遅延補完データと、a(n)で受信した即時補完データの合併は、a(n)のST2における全ての認証パスノードの割当値を含んでいる。

【０２８３】

（２）帰納ステップ

i1∈{0, …, n－i} とし、i＝i1としたとき、手順COMPLETION-BULK-BACKWARD1により追加されたものを含むa(n－i) の遅延補完データと、a(n－i)で受信した即時補完データの合併は、a(n－i) のST2における全ての認証パスノードの割当値を含んでいるものと仮定する。 i ＝i1＋1 に対しても同じことが成立つことを示せばよい。このことは、以下のように完全化波及処理を用いることにより示すことができる。

【０２８４】

a2＝ a(n－i1)、a1＝a(n－(i1＋1)) とおき、 a1 のa2による認証点を AP(a1, a2)、その兄弟ノードを AP'(a1, a2)、さらにAP(a1, a2) のレベルをj1と置く（図37を参照）。

【０２８５】

以下で述べる順次集約木の性質により、順序集約小木ST2におけるa1のST2における認証パスノードのうちレベルがj1 より小さいもの割当値は、図35のステップST5004において追加されるデータに含まれる。

【０２８６】

a1のST2における認証パスノードのうちレベルがj1に等しいものの割当値は、図35のステップST5007において追加されるデータに含まれる。

【０２８７】

a1のST2における認証パスノードのうちレベルがj1より大きいものの割当値は、図35のステップST5008において追加されるデータに含まれる。

【０２８８】

以上により、手順COMPLETION-BULK-BACKWARD1により追加されたものを含むa1＝a(n－(i＋1)) の遅延補完データとa(n－(i＋1)) で受信した即時補完データの合併は、a(n－(i＋1))のST2における全ての認証パスノードの割当値を含むことが導かれる。

【０２８９】

以上（１）及び（２） により、 i＝0, …, n について、手順COMPLETION-BULK-BACKWARD1により追加されたものを含むa(n－i) の遅延補完データと、a(n－i)で受信した即時補完データの合併は、a(n－i) のST2における全ての認証パスノードの割当値を含んでいることが示される。

【０２９０】

なお、同様の帰納法により、図35のステップST5006で判定結果が NO となり、エラーとなることはないことも示される。

【０２９１】

（メモリの効率化）

上記は、１つの集約間隔において連鎖補完方式により利用者装置51がイベント順序証明応答として取得したデータを計算機のメモリに読み込むことができるできる場合の処理方式である。 集約間隔における利用者装置51による登録点が多数に上り上記の取得データを計算機のメモリに読み込むことができない場合には、以下の方式により取得データの一部をメモリに読み込み、完全認証パスデータを段階的に計算することにより、当該の集約間隔における全ての登録点の完全認証パスデータを計算することができる。

【０２９２】
上記の計算は、以下のステップ(1)及至(5)により行われる。
【０２９３】
(1) ある集約間隔にある利用者装置51が受信した補完データのうちから、登録点のインデックスが特定の条件を満たすもののみを間引き抽出し、間引き抽出データを構成する。
【０２９４】
間引き抽出するための条件として、間引き間隔となる正整数m を指定し、登録点のインデックスが m で割り切れるもののみを抽出することにしてもよい。図38に示す具体例においては、インデックス 0から10までをもつ登録点（黒い点で示されている）から、間引き間隔を5 として、5で割り切れるインデックス即ち0，5，10を持つ登録点を抽出し、間引き抽出データを構成している。
【０２９５】
(2) 登録点のインデックスが隣あう間引き抽出データのインデックスで挟まれているような登録点の登録値および補完データからなる局所データを構成する。このような局所データは、一般には複数構成される。
【０２９６】
図39に示す具体例においては、間引き抽出データの1番目のインデックス0と2番目のインデックス5に挟まれたインデックスを持つ登録点を集め第１の局所データを構成している。図40に示す具体例においては、間引き抽出データの2番目のインデックス5と3番目のインデックス10に挟まれたインデックスを持つ登録点を集め第2の局所データを構成している。
【０２９７】
(3) 上記(2)で構成された各局所データを、その局所データの最も右に位置する登録点を暫定終端点として扱い、前記のインクリメンタル完全化の処理を行う。この処理を局所データの局所完全化と呼ぶ。
【０２９８】
この処理により計算される遅延補完データを用いて、当該の局所データに属する登録点のうち最も右に位置するものをa1 としたとき、当該の局所データに属する各登録点a について， a のa1による認証点をAP(a，a1)としたとき，aの認証パスノードの中で、level(AP(a，a1))より低いレベルのものに対しては、その割当値を計算することができる。さらに、ここで割当値を計算できるaの認証パスノードの割当値は、 a の認証パスノードのうちa1の処理が終了した時点で割当値が定まっているもの全てを含んでいる。即ち、登録点a のa1 時点の遅延補完データを含んでいる。
【０２９９】
図39に示す具体例においては、この局所データの局所完全化の処理により、インデックス0の登録点の遅延補完データとして、ノード(1，0)，(2，1) の割当値が計算され、インデックス1の登録点の遅延補完データとして、ノード(2，1)の割当値が計算され、インデックス3の登録点の遅延補完データとして、ノード(1，5)の割当値が計算される。
【０３００】
この局所データに属する登録点のうち最も右に位置するものはインデックス5の登録点でありこれをa1と置くと、この局所データに属する各登録点aについて、level(AP(a，a1))より小さいレベルの認証パスノードの割当値が計算できる。例えば、a をインデックス0の登録点とすると、AP(a，a1) は(3，0) であり、a の認証パスノードのうちレベルが 3 より小さいもの (0，0)，(1，0)，(2，1) の割当値を計算できる。a のa1における遅延補完データは(1，0)，(2，1) の割当値であるので、a1時点における遅延補完データは計算できることがわかる。この局所データに属する他の登録点についても同様である。
(4) 上記(3)の処理の結果、間引き抽出データの隣あう２つの登録点a1 と a2 について、a1 のa2時点における遅延補完データを取得することが出来る。このデータを用いて前記の証明書完全化のメインルーチン COMPLETION-MAIN1 を適用し、間引き抽出データに含まれる各登録点で取得する証明書の完全化、即ち該登録点の全ての認証パスノードの割当値

を計算する。この処理を間引き抽出データの大域完全化と呼ぶ。

【０３０１】

図41で示す具体例においては、間引き抽出データのインデックス0，1，2の登録点、即ち、リーフ番号1，11，31の登録点の証明書の完全化を行い、当該の3つの登録点の全ての認証パスノードの割当値を計算することができる。例えば、間引き抽出データのインデックス0の登録点の認証パスノードは (0，0)，(1，1)，(2，1)，(3，1)，(4，1) であるが、これら全ての割当値を計算することができる。

【０３０２】

(5) 上記(3)で構成した局所完全化された局所データの各々と、上記(4)で構成した大域完全化された間引き抽出データを用いて、当該の局所データに含まれる各登録点で取得する証明書の完全化を行う。この処理を局所データの大域完全化と呼ぶ。

【０３０３】

局所データの大域完全化の手順は、詳しくは以下の通りである。

【０３０４】

(5-1) ある局所データの登録点を a(0)，a(1)，…，a(n)＝al とするとき、al の全ての認証パスノードの割当値は、ステップ(4) で計算済みである。これを、

V(0)，V(1)，…，V(k－1) とする。

【０３０５】

(5-2) 従って、al のルートパスに属する各ノードの割当値も計算できる。これを

V'(0)，V'(1)，…，V'(k－1)，V'(k) とする。

【０３０６】

(5-3) 各 a ＝ a(0)，…，a(n－1) について、a の al による認証点をAP(a，al)とし、kl ＝ level(AP(a，a(n)) とおく。

【０３０７】

(5-4) ステップ(3) により、a の認証パスノードのうちレベルがklより小さいものの割当値は計算可済みである。

【０３０８】

(5-5) また、レベルがklのaの認証パスノードはalのルートパスに属するノードでレベルがklのものと一致する。従って、このような認証パスノードの割当値は、上記 (5-2) で計算したV'(kl) となる。

【０３０９】

(5-6) kl ＜ j ＜ kとなるjについて，aの認証パスノードのうちレベルがjのものは、alの認証パスノードのうちのレベルがj のものと一致する。従って、その認証パスノードの割当値は、上記 (5-1) で計算した，V'(j) である。

【０３１０】

以上、(5-1) 及至(5-6) により、各 a ＝ a(0)，…，a(n－1) についてa の全ての認証パスノードの割当値を計算することが出来る。

【０３１１】

図39 で示す具体例について言えば、インデックス2の登録点（リーフ識別番号5）の認証パスノードは、(0，4)，(1，3)，(2，0)，(3，1)，(4，1) である。また alをインデックス5の登録点(リーフ識別番号11)とすると、AP(a，al)＝ (3，0) であり、kl＝ level(AP(a，al)) ＝ 3 である。a の認証パスノードのうちレベルがkl＝3 より小さい (0，4)，(1，3)，(2，0) についてはそれらの割当値は、上記ステップ(5-3) で計算できる（図39、図42参照）。また，レベルがkl＝3 の認証パスノード(3，1) の割当値は(5-2)で計算できる（図41、図42参照）。また、レベルがkl＝3より大きい(4，1) についてはステップ(5-1)で計算できる（図41、図42参照）。

以上のステップ(1)及至(5)の手順により、取得した証明書の完全化を行うために、同時にメモリ上に保持する必要のあるデータは、間引き抽出データと、一つの局所データのみである。登録点の総数をN とし，上記ステップ(1)で用いる間引き間隔をm とすると、同時にメモリ上に保持する必要がある登録点の数は、(N/m) ＋ m となる。m＝ √N とする

と、 (N/m) ＋ m ＝ 2・√N となり、必要なメモリ容量のオーダを N から √N に削減することが可能となる。

【０３１２】

＜２－５．利用者装置51の補完データによるルート値計算＞

次に、利用者装置51の補完データによるルート値計算について、説明する。これは、利用者装置51の第１の検証機能におけるルート値計算について詳しく説明するものである。

【０３１３】

ある集約間隔I1が終了したとき、利用者装置51は、集約間隔I1の間に送信した１つの証明要求RQ に対する受理証明書の個別完全化を上述の方法で実行することにより、完全認証パスデータを計算することができる。完全認証パスデータから、以下に示す（１）乃至（５）に示す手順により、当該の集約間隔の順次集約木のルートの割当値が計算できる。

【０３１４】

まず完全認証パスデータは、即時補完データと遅延補完データからなる。即時補完データや遅延補完データは、（位置情報，ＬＲタグ，割当値（ハッシュ値））で示す形式の補完データ要素からから成るものとする。尚、ＬＲタグはＬというタグかＲというタグのどちらかの値をとる。ここで、上記の位置情報はレベル情報を含むものとする。レベル情報の間には以下のような２項関係＜＜が定義されているものとする。

【０３１５】

任意の登録点について、その完全認証パスデータに含まれる補完データ要素を

(位置情報P(i)，ＬＲタグT(i)，割当値H(i)) （但し，i ＝1，…，n）

とし、位置情報P(i) に含まれるレベル情報を level(P(i)) と表すと、２項関係 ＜＜は

level(P(1))，…，level(P(n))

の間に線形順序を定義するものとする。

【０３１６】

位置情報を１つの集約木におけるレベル（非負整数で表される）とレベル内のインデックスの組み合わせとし、位置情報のうちレベル情報は組み合わせの第１要素とすると、上記２項関係＜＜としては、整数の大小関係＜をとればよい。

【０３１７】

図43は、完全認証パスデータによる順次集約木のルート値の計算方法を示すフローチャートである。同図によれば、完全認証パスデータのチェック、即ち、即時補完データはＬタグ、遅延補完データはＲタグを有するかのチェック、及び完全認証パスデータに重なるレベル情報がないかのチェックを確認した後、レベル情報の順序でソートし、各割当値をＬＲタグに合わせて連接して、ルート値を計算する（ステップS3101，S3102，S3103，S3104，S3105，S3106）。

【０３１８】

次に、図44及び図45に示すように、ある集約間隔の順次集約木のリーフの１つとして、前の集約間隔の順次集約木のルート値を取り入れる場合について説明する。このような場合には、異なる順次集約木間における受理証明書発行の時間的前後を検証することが簡単にできるという効果がある。例えば、図45において、利用者装置2Aの登録点aが順次集約木ST(5)の部分木ST1(5)のリーフに割り当てられており、また、利用者装置2Bの登録点bが順次集約木ST(6)の部分木ST1(6)のリーフに割り当てられているときは、aとbの合流点がノードR(6)、aのbによる認証点がノードR(5)になるので、登録点aから計算された認証点R(5)の値が、登録点bの即時補完データに含まれていれば、登録点aの登録は登録点bの登録より時間的に前であることを検証することができる。

【０３１９】

図44は、図45のように複数の順次集約木がリンクされた状況において、１つの順次集約木ST(n)を抽出したものである。

【０３２０】

ここで、ルートR(n-1)は、順次集約木ST(n－1)と順次集約木ST(n)に共通するノードで

レベル情報 (L, TID(n−1), k(n−1))
レベル内 index 0
位置情報 ((L, TID(n−1), k(n−1)), 0)
である。尚、上述のレベル情報は、
(LRタグ，非負整数の集約木番号，非負整数の集約木内のレベル情報)
で表現されており、LRタグは、Lというタグと Rというタグのとちらかの値をとる。

【０３２１】

また、部分木 STl(n) のルート Rl(n)は、
レベル情報 (R, TID(n−1), kl(n))
レベル内 index l
位置情報 ((R, TID(n−1), kl(n)), l)
であり、ここで、kl(n) はSTl(n) の高さである。

【０３２２】

また、部分木STl(n) に関しては、
ルート Rl(n)以外のノードについては、レベル情報 (R, TID(n), j)
ルートRl(n)以外のノードの位置情報は((R, TID(n), j), i) である。

【０３２３】

ここで，j，i は非負整数であり、leafs(STl(n)) の各要素の位置情報は((R, TID(n), 0), i) と表すことができる。

【０３２４】

また、 R(n)は順次集約木ST(n) とST(n＋l)に共通するノードで、
レベル情報 (L, TID(n), k(n))
レベル内 index 0
位置情報 ((L, TID(n), k(n)), 0)　　（但し、 k(n) ＝ kl(n) ＋l とする）
割当値 V(R(n)) ＝ h(V(R(n−l)) ‖ V(Rl(n)))
である。
また、 順次集約小木 STl(n) とルートR(n−l)、 ルートR(n) からなる二分木をST(n) と書く。即ち、
root(ST(n)) ＝ R(n)、
leftChild(R(n)) ＝ R(n−l)、
rightChild(R(n)) = Rl(n)。

【０３２５】

第n番目の集約期間に対応する順次集約木は ST(n) である。

【０３２６】

但し、 n＝0 に対しては、R(n−l) の代わりに所定の割当値を持ったノードIRを用いる（図45参照）。IR の位置情報は ((L, −l, 0), 0) である。

【０３２７】

このとき、２つの 拡張レベル情報の間の順序＜＜を次のように定義する。

【０３２８】

∀jl, j2 , Tl, T2 ≧0[(R, T2, j2) ＜＜ (L, Tl, jl)] 、
∀jl, j2, Tl, T2≧0[Tl＜T2 ⇒ (L, Tl, jl) ＜＜ (L, T2, j2)]、
∀jl, j2, Tl≧0[jl ＜j2 ⇒ (R, Tl, jl) ＜＜ (R, Tl, j2)]。

【０３２９】

この定義により、二項関係＜＜は任意の登録点の認証パスノードの集合に線形順序を定めるものであることが導かれる。

【０３３０】

図46は、この定義された２項関係＜＜を用いて補完データによる集約木ルート値を計算する一例を示すもので、計算は以下のようになる。

【０３３１】

位置情報 ((R, 10, 0), 5) のノードに対して、即時補完データは、

[(((L, 9, k(9)), 0), L, V(R(9))),
(((R,10, 2), 0) , L, V((R, 10, 2), 0)),
(((R, 10, 0), 4), L, V((R, 10, 0), 4))]
となる。ここで (R, 10, 2) ＜＜ (L, 9, 10) である。

【０３３２】

遅延補完データは、[(((R, 10, 1), 3), R, V((R, 10, 1), 3))]
補完データからのルート値の計算を図43のフローに従って行う。

【０３３３】

(1) 即時補完データの各要素はLタグを持つことをチェックする→ 合格
(2) 遅延補完データの各要素はRタグを持つことをチェックする→ 合格
(3) 即時補完データと遅延補完データを合併する
合併結果は、
[(((L, 9, k(9)), 0), L, V(R(9))),
(((R,10, 2), 0) , L, V((R, 10, 2), 0)),
(((R, 10, 0), 4), L, V((R, 10, 0), 4)) ,
(((R, 10, 1), 3), R, V((R, 10, 1), 3))]
となる。

【０３３４】

(4) 合併結果の中に、重なるレベル情報がないことを確認する→合格
(5) 合併結果を、レベル情報の順序＜＜基準にソートする
ソート結果は，
[(((R, 10, 0), 4), L, V((R, 10, 0), 4)) ,
(((R, 10, 1), 3), R, V((R, 10, 1), 3)),
(((R,10, 2), 0) , L, V((R, 10, 2), 0)),
(((L, 9, k(9)), 0), L, V(R(9)))]
となる。

【０３３５】

(6) ステップ(5) のソートの結果を
(J(0), LR(0), V(0)), …, (J(k－1), LR(k－1), V(k－1))
とおき、当該の登録点の登録値を V(0) とおき、以下のように再帰的に
W(0), W(1), …, W(k－1), W(k)
を定義する。

【０３３６】

(i)W(0) ＝ V(0)
(ii) LR(j) ＝ L のとき，W(j＋1) ＝ h(V(j)‖W(j))
LR(j) ＝ R のとき、 W(j＋1) ＝ h(W(j) ‖V(j))
これに従って計算すると、k ＝4 であり、W(j) は以下のように計算できる。

【０３３７】

W(0) = V((R, 10, 0), 5).
W(1) = h(V((R, 10, 0), 4) ‖V((R, 10, 0), 5)),
W(2) = h(W(1) ‖ V((R, 10, 1), 3)),
W(3) = h(V((R, 10, 2), 0) ‖W(2)),
W(4) = h(V(R(9)) ‖W(3))
となる。W(3) = V(R1(10)) 、W(4) = V(R(10)) である。

【０３３８】

従って、第２の実施の形態のイベント順序証明システム200によれば、第１の実施の形態と同じ効果を得ることができる。即ち、木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、利用者装置51から証明要求を受付けた証明装置4が、該証明要求に対して受理証明書を含む連鎖補完方式（登録点に関して、登録点の即時補完データ及び直前登録点の登録点における遅延補完データを証明応答データに含む）による証明

応答を発行したときでも、利用者装置21がこの証明応答を用いて、インクリメンタル完全化を行うと、利用者装置21間における受理証明書発行の時間的前後を検証することができるので、証明要求をまとめた公表データが電子的に公表される前であっても、受理証明書の正当性を検証することができる。

【０３３９】

また、連鎖補完方式には、シーケンス補完方式よりも、証明応答のデータ量が少なくて済むという効果がある。さらには、連鎖補完方式においても、証明装置4は、順次集約木そのものを記憶部に記憶させる方法は勿論、スタック構造を用いた記憶方法も用いることができるので、証明装置4の必要記憶容量を大幅に減少させることもできる。

【０３４０】

また、利用者装置51におけるインクリメンタル完全化処理においても、個別完全化及び一括完全化の双方を具備するので、状況に応じて最適なインクリメンタル完全化を行うことにより、受理証明書の正当性を検証することができる。さらに、証明応答データすべてを利用者装置51のメモリ上に記憶させず、部分的な局所データだけを記憶させる方式であっても、インクリメンタル完全化を行うことができるので、利用者装置51の必要なメモリ量を大幅に減少させることができる。

【０３４１】

また、順次集約期間が終了後においては、利用者装置51は、インクリメンタル完全化の処理により、完全補完データを取得できるので、順次集約木のルート値を計算することができる。さらに、前の集約間隔の順次集約木のルート値を次の順次集約木のリーフの割当値とする場合には、順次集約木をまたがった受理証明書発行の時間的前後を検証することが簡単にできる。

【０３４２】

以上、本発明の実施例について説明してきたが、本発明の要旨を逸脱しない範囲において、本発明の実施例に対して種々の変形や変更を施すことができる。例えば、上記実施の形態においては、順次集約木として二分木を用いたが、本発明は二分木に限定されるものではなく、１つの親が複数の子を持つ有向木であればよいものである。

【０３４３】

また、利用者装置21又は51は、一定時間間隔終了前に、証明装置１又は４が運用を中断、あるいは順次集約木のルート値を計算するのに必要なデータを消失したとき、証明装置１又は４の運用中断あるいはデータ消失の時点までに受信し記憶した順序証明応答から、計算可能な割当値を持つ順次集約木のノードのうちで、その親のノードの割当値が計算できないような１つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表手段を有してもよい。そして、この場合、所定の検証機関が、この公表情報が矛盾しないことを検証するようにしてもよい。

【０３４４】

＜順次集約木の性質＞

上記実施の形態で用いた順次集約木の性質について詳しく説明する。

【０３４５】

順次集約木のリーフ番号iについて、iで識別される順次集約木のリーフに順次割当値を割り当てる元となった証明要求を受付けて該リーフに割当値を割り当てる一連の処理を該リーフに対する処理ラウンドと言いround(i) と表す。

【０３４６】

今、甲 を利用者装置、Ｚ を監査装置とし、i0 と i1 を i0 ＜ i1 なる二つの順次集約木リーフ番号とし、round(i0) において甲は受理証明書を受信し、Ｚ はround(i1) において監査用受理証明書を受信したものとする。このとき、i0 の i1 による認証点は以下の性質を持つ。

【０３４７】

（１）認証点の割当値は、監査点、即ちノード（0，i1）の即時補完データに含まれる。

【０３４８】

（２）上記認証点を(j', i') とおき、round(jl) 終了時にリーフ(0, i0) が属する順次集約小木をST2とし、(0, i0) のST2における認証パスを$authPath_{ST2}$(0, i0))としたとき、$authPath_{ST2}$(0, i0))に属するノードで、レベルがj'より小さいものに対する割当値は、ノード（0, i0）に対応するラウンドで受理証明書を受理した利用者が、ノード（0, il）に対応するラウンド以降において受信できる遅延補完データあるいは受信した即時補完データに含まれる。

【０３４９】

即ち、il ≦ i2 とすると、$authPath_{ST2}$(0, i0)) に属するノードで、レベルがj'より小さいものに対する割当値は、immedData(i0) あるいはlateData(i0, i2) に含まれる。

【０３５０】

（３）ST2におけるリーフ(0, i0) のルート・パスを$rtPath_{ST2}$(0, i0)としたとき、上記認証点の割当値及び$rtPath_{ST2}$(0, i0)属するノードでレベルが該認証点のレベルより小さいノードの割当値は、ノード（0, i0）で受理証明書を受理した利用者が、ノード（0, il）に対応するラウンド以降において受信する遅延補完データおよびノード(0, i0)で受信した受理証明書（即時補完データを含む）から計算することができる。

【０３５１】

（性質の証明）

以下では、利用者に渡す受理証明書に、即時補完データを含める場合について説明する。利用者に渡す受理証明書に即時補完データを含めず、その代わりに遅延補完データにこの情報を含める場合でも同様の議論により同じ結論が得られる。

【０３５２】

（１） まず、項目（1）について図47、図48を用いつつ説明する。

【０３５３】

（場合１）最初に、図47を参照して、i0 とil がil時点における順次集約フォレスト内の１つの順次集約小木ST2に属する場合を考える。ここで、合流点を（j, i）、そのレフト・チャイルドである認証点を（j', i'）とおく。ノード（0, il）の順次集約小木ST2 におけるルート・パス $rtPath_{ST2}$(0, il)において、（0, il）から出発して、合流点に至る直前のノードを（j", i"）とおく。このとき、認証点は、（j", i"）の左補完点である。従って、認証パス $authPathT_{ST2}$(il)の定義から、((j', i'), L)はノード（0, il）のST2 における認証パスに含まれる。また、ノード(j', i')への値の割当ては、round(il)より前に終了している。 よって、((j', i'), L, V(j', i'))は（0, il）に対する即時補完データに含まれる。

【０３５４】

（場合２）次に、図48を参照して、i0 とil がil時点における順次集約フォレスト内のとの順次集約小木にも同時には属さない場合を考える。このとき、i0 はil時点における順次集約フォレスト内のある順次集約小木ST2' に属する。このとき、登録点(0, il)に対する即時補完データの定義により、V(root(ST2')) は、登録点(0, il) に対する即時補完データに含まれる。

【０３５５】

（２） 次に項目（２）について図49乃至52を用いつつ説明する。

【０３５６】

（場合１）最初に、図49及び50を参照して、i0 とil がil時点における順次集約フォレスト内の１つの順次集約小木ST2に属する場合を考える。

【０３５７】

k = height(ST2) とおく。

【０３５８】

認証点（j', i'）はノード（0, i0）のルート・パス $rtPath_{ST2}$(0, i0) に含まれる。ここで、

$rtPath_{ST2}(0, i0) = [(0, r(0)), \cdots, (j', r(j')), (j'+1, r(j'+1)), \cdots, (k, r(k))]$

とする。また，$authPath_{ST2}(0, i0)$ の要素で、レベルがj'より小さいノードの並びを
[(0, s(0)), …, (j'－1, s(j'－1))]
とおく。各j1 ∈ [0..j'－1] に対して、V(j1, r(j1)) がimmedData(i0)あるいはlateData(i0, i2) に含まれることを示せばよい。

【０３５９】

$authPath_{ST2}(0, i0)$の定義により、$authPath_{ST2}(0, i0)$のレベル j1の要素 p2＝(j1, s(j1))は、$rtPath_{ST2}(0, i0)$)のレベルj1＋1の要素 p3＝(j1+1, r(j1+1))のライト・チャイルドであるか或いはレフト・チャイルドである。とちらであるかによって場合分けする。

【０３６０】

（場合１－１） p2がp3のライト・チャイルドであるとき、図49に示すように、 p2の割当値V(p2)は、i1≦i2なるi2において、甲が受信できる遅延補完データ lateData(i0, i2) に含まれる。なぜならば、リーフ(0, i1) に対応するラウンドのイベント順序証明処理が終わった時点で、図49のBで表された SB2 の部分木の割当値は計算可能であり計算され割当て済みである。従って、その時点以降で発行される登録点i0に対する遅延補完データにはBのルートp2の割当値V(p2) が含まれるからである。

【０３６１】

（場合１－２）p2がp3のレフト・チャイルドであるとき、図50に示すように、ノードp2の割当値V(p2)は、登録点i0に対する即時補完データに含まれる。何故ならば、図50 の p1 をルートとする部分木B について、
∀i∈leafs(B)[i ＜ i0]
であり、従ってi0で識別されるラウンドの開始時に、leafs(B)の割当値は確定している。よって、p2 ＝ root(B)の割当値は、i0で識別されるラウンドにおいて確定しており、従ってp2 はi0 時点において値が確定しているi0の認証パスノードの集合に含まれるからである。

【０３６２】

（場合２）次に、図51及び図52を参照して、i0 とi1 がi1時点における順次集約フォレスト内のとの順次集約小木にも同時には属さない場合を考える。このとき、i0 はi1時点における順次集約フォレスト内のある順次集約小木ST3に属し、root(ST3) がi0 のi1による認証点となる。k＝height(ST3) と置く。認証点 (j', i') は(0, i0)のルートパス $rtPath_{ST3}(0, i0)$ に含まれる。ここで、
$rtPath_{ST3}(0, i0)$＝ [(0,r(0)), …, (j',r(j')), (j'＋1, r(j' ＋1)), …, (k, r(k))]
とする。また、$authPath_{ST3}(0, i0)$ の要素で、レベルがj'より小さいノードの並びを
[(0, s(0)), …, (j'－1, s(j'－1))]
とおく。各j1 ∈ [0..j'－1] に対して、V(j1, r(j1)) がimmedData(i0)あるいはlateData(i0, i2)に含まれることを示せばよい。

【０３６３】

$authPath_{ST3}(0, i0)$の定義により、$authPath_{ST3}(0, i0)$のレベル j1の要素 p2＝(j1, s(j1))は，$rtPath_{ST3}(0, i0)$)のレベルj1＋1の要素 p3＝(j1+1, r(j1+1))のライト・チャイルドであるか或いはレフト・チャイルドである。どちらであるかによって場合分けする。

【０３６４】

（場合２－１） p2がp3のライト・チャイルドであるとき、図51に示すように、p2の割当値V(p2)は、i1≦i2なi2において、甲が受信できる遅延補完データ lateData(i0, i2) に含まれる。なぜならば、リーフ(0, i1) に対応するラウンドのイベント順序証明処理が終わった時点で、図51のBで表された SB3 の部分木の割当値は計算可能であり計算され割当て済みであり、従ってその時点以降で発行される登録点i0に対する遅延補完データにはBのルートp2の割当値V(p2)が含まれるからである。

【０３６５】

（場合２－２）p2がp3のレフト・チャイルドであるとき、図52に示すように、ノードp2の割当値V(p2)は、登録点i0に対する即時補完データに含まれる。何故ならば、図52のp1をルートとする部分木B について、

$$\forall i \in leafs(B)[\ i < i0\ ]$$

であり、従ってi0で識別されるラウンドの開始時に、leafs(B)の割当値は確定している。よって、p2 ＝ root(B)の割当値は、i0で識別されるラウンドにおいて確定しており、従ってp2 はi0 時点において値が確定しているi0の認証パスノードの集合に含まれるからである。

【０３６６】

（３） 認証パスの定義及び項目(2)から、各$j1 \in [0..j']$に対して、V(j1, r(j1)) を以下のように再帰的に計算することが出来る。

【０３６７】

まず、V(j1, r(j1)) は受理証明書に含まれているノード(0, i0) の割当値とする。

【０３６８】

次に、$j1 \in [0..j'-1]$に対して、V(j1, r(j1)) が計算されたと仮定し、V(j1+1, r(j1+1))を以下のように計算する。r(j1) ＜ s(j1) のときは、

$$V(j1+1,\ r(j1+1)) = h(V(j1,\ r(j1)) \| V(j1,\ s(j1)))$$

とし、s(j1) ＜ r(j1) のときは、

$$V(j1+1,\ r(j1+1)) = h(V(j1,\ s(j1)) \| V(j1,\ r(j1)))$$

とする。

【図面の簡単な説明】

【０３６９】

【図１】本発明の第１の実施の形態に係るイベント順序証明システムのシステム構成図である。

【図２】本発明の第１の実施の形態に係るイベント順序証明システムに用いられる順次集約木の構成を説明する図である。

【図３】本発明の第１の実施の形態に係るイベント順序証明システムのイベント順序受理証明書の構成を示す図である。

【図４】本発明の第１の実施の形態に係るイベント順序証明システムにおいて各登録点とその補完データを説明する図である。

【図５】本発明の第１の実施の形態に係るイベント順序証明システムの利用者装置におけるイベント順序の判定方法を説明する図である。

【図６】本発明の第１の実施の形態に係るイベント順序証明システムのイベント順序証明方法の動作を説明するシーケンス図である。

【図７】本発明の第１の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法の動作を説明するシーケンス図である。

【図８】本発明の第１の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法の動作を説明するシーケンス図である。

【図９】本発明の第２の実施の形態に係るイベント順序証明システムのシステム構成図である。

【図１０】本発明の第２の実施の形態に係るイベント順序証明システムのイベント順序受理証明書の構成を示す図である。

【図１１】本発明の第２の実施の形態に係るイベント順序証明システムにおける完全化波及処理を説明する図である。

【図１２】本発明の第２の実施の形態に係るイベント順序証明システムにおいて完全化波及処理を用いることにより、連鎖補完方式の証明応答からシーケンス補完方式の証明応答を計算できることを示す図である。

【図１３】本発明の第２の実施の形態に係るイベント順序証明システムにおいて第１の連鎖補完方式を説明する図である。

【図１４】本発明の第２の実施の形態に係るイベント順序証明システムにおいて第１

の連鎖補完方式による証明応答作成の動作を説明するフローチャートである。
【図１５】本発明の第２の実施の形態に係るイベント順序証明システムにおいて第２の連鎖補完方式を説明する図である。
【図１６】本発明の第２の実施の形態に係るイベント順序証明システムにおいて第２の連鎖補完方式による証明応答作成の動作を説明するフローチャートである。
【図１７】本発明の第２の実施の形態に係るイベント順序証明システムの第２の連鎖補完方式におけるデータ構造の一例である。
【図１８】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式における即時補完データ及び遅延補完データの計算手順の一例を説明するフローチャートである。
【図１９】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるノード値計算順の一例を説明するフローチャートである。
【図２０】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式における遅延データ設定手順の一例を説明するフローチャートである。
【図２１】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式における順次集約木の切替処理の一例を説明するフローチャートである。
【図２２】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式における順次集約木の終端・切替処理のサブルーチンの一例を説明するフローチャートである。
【図２３】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式における順次集約木の切替処理のサブルーチンの一例を説明するフローチャートである。
【図２４】図２２の処理を具体的に説明する図である。
【図２５】順次集約フォレストと順次集約小木を説明する図である。
【図２６】順次集約フォレストと現時点順次集約木を説明する図である。
【図２７】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全個別化の動作を説明するフローチャートである。
【図２８】図２７の処理を具体的に説明する図である。
【図２９】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全個別化の順次集約小木決定の計算手順の一例を説明するフローチャートである。
【図３０】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル個別完全化の取得参照点決定の計算手順の一例を説明するフローチャートである。
【図３１】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル個別完全化の連鎖補完データ蓄積用データ構造の一例である。
【図３２】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル個別完全化のアルゴリズムを説明する図である。
【図３３】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル個別完全化の認証パスノードの割当値の計算手順の一例を説明するフローチャートである。
【図３４】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル個別完全化の認証パスノードの各割当値の計算手順の一例を説明するフローチャートである。
【図３５】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル一括個別化の手順の一例を説明するフローチャートである。
【図３６】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル一括個別化の根拠を説明する図である。

【図３７】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル一括個別化の根拠を説明する図である。
【図３８】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全化（一部をメモリに納め、多段式に実行する方式）を説明する図である。
【図３９】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全化（一部をメモリに納め、多段式に実行する方式）を説明する図である。
【図４０】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全化（一部をメモリに納め、多段式に実行する方式）を説明する図である。
【図４１】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全化（一部をメモリに納め、多段式に実行する方式）を説明する図である。
【図４２】本発明の第２の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全化（一部をメモリに納め、多段式に実行する方式）を説明する図である。
【図４３】完全認証パスデータによる順次集約木のルート値の計算方法を示すフローチャートである。
【図４４】ある集約間隔の順次集約木のリーフの１つとして、前の集約間隔の順次集約木のルート値を取り入れる場合の順次集約木を説明する図である。
【図４５】ある集約間隔の順次集約木のリーフの１つとして、前の集約間隔の順次集約木のルート値を取り入れる場合の順次集約木を説明する図である。
【図４６】ある集約間隔の順次集約木のリーフの１つとして、前の集約間隔の順次集約木のルート値を取り入れる場合の完全認証パスデータによる順次集約木のルート値の計算方法を説明する図である。
【図４７】認証点の割当値は、監査点の受理証明書内補完データに含まれることを説明する図である。
【図４８】認証点の割当値は、監査点の受理証明書内補完データに含まれることを説明する図である。
【図４９】認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。
【図５０】認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。
【図５１】認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。
【図５２】認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。
【図５３】イベント順序証明システムの概念を説明する図である。
【図５４】線形リンキングを用いたイベント順序証明システムの概念を説明する図である。

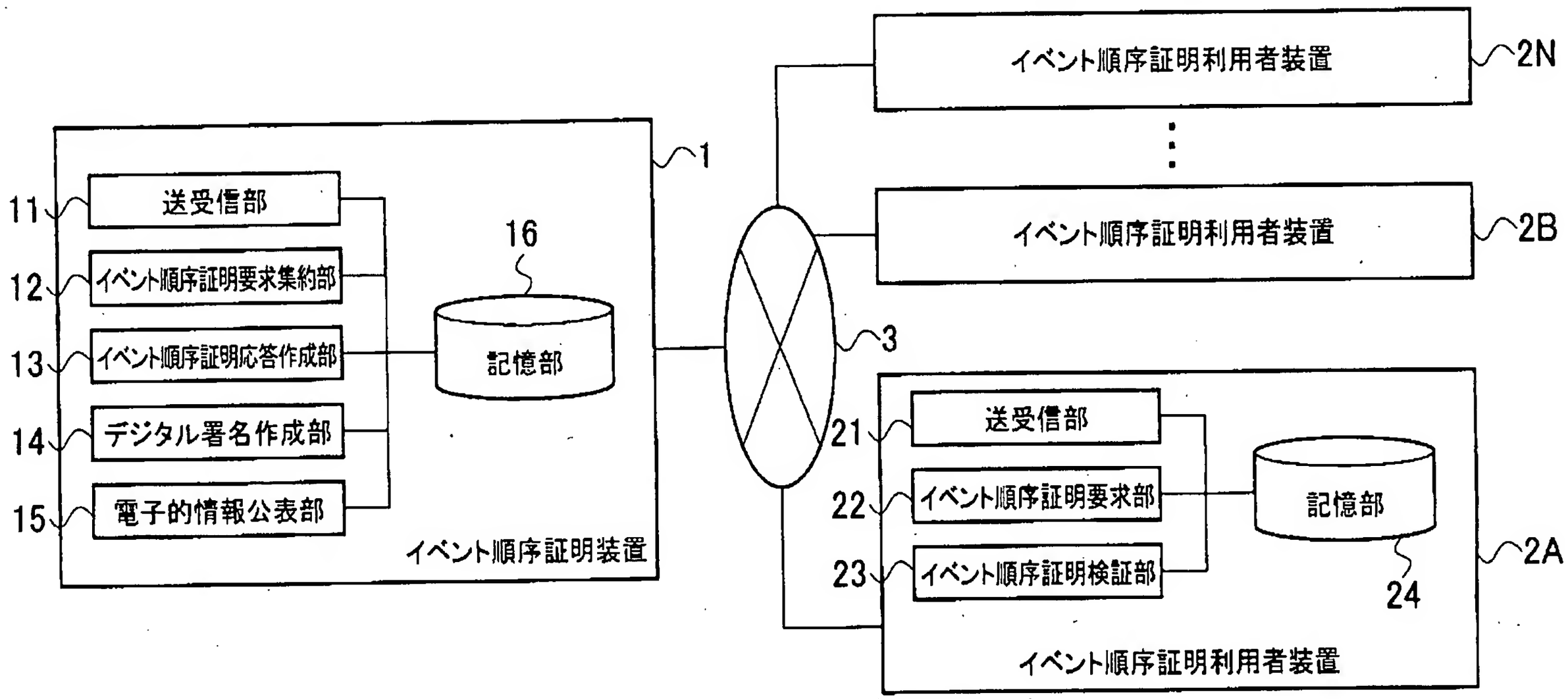
【符号の説明】

【０３７０】

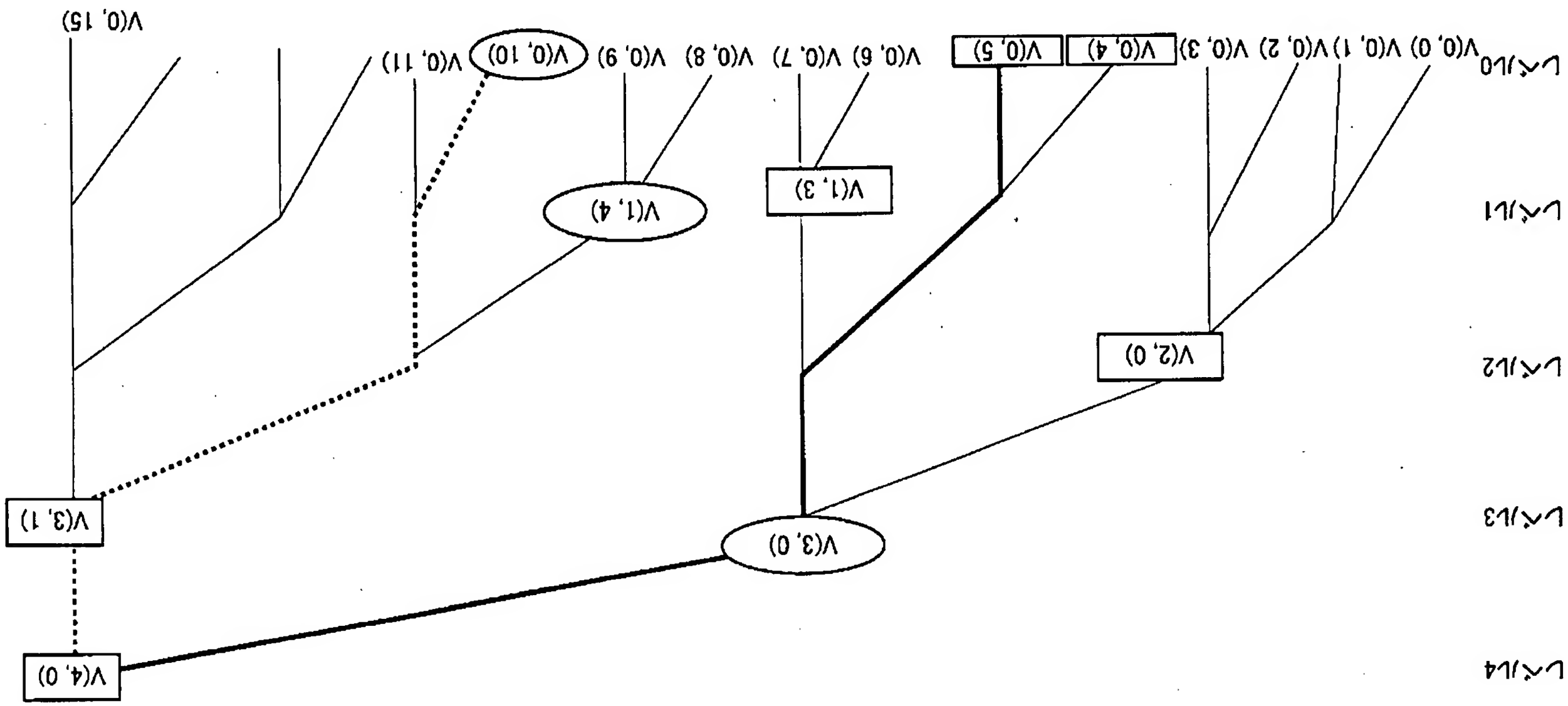
１，４…イベント順序証明装置
２Ｉ，５Ｉ…イベント順序証明利用者装置
３…コンピュータネットワーク
１１，２１…送受信部
１２…イベント順序証明要求集約部
１３，４１…イベント順序証明応答作成部
１４…デジタル署名作成部

１５…電子的情報公表部
１６，２４，４２…記憶部
２２…イベント順序証明要求部
２３，５１…イベント順序証明検証部
１００，２００…イベント順序証明システム

【書類名】 図面
【図１】


1
11
送受信部
12
イベント順序証明要求集約部
13
イベント順序証明応答作成部
14
デジタル署名作成部
15
電子的情報公表部
16
記憶部
イベント順序証明装置
イベント順序証明利用者装置
2N
イベント順序証明利用者装置
2B
3
21
送受信部
22
イベント順序証明要求部
23
イベント順序証明検証部
記憶部
24
2A
イベント順序証明利用者装置
100 イベント順序証明システム

【図２】

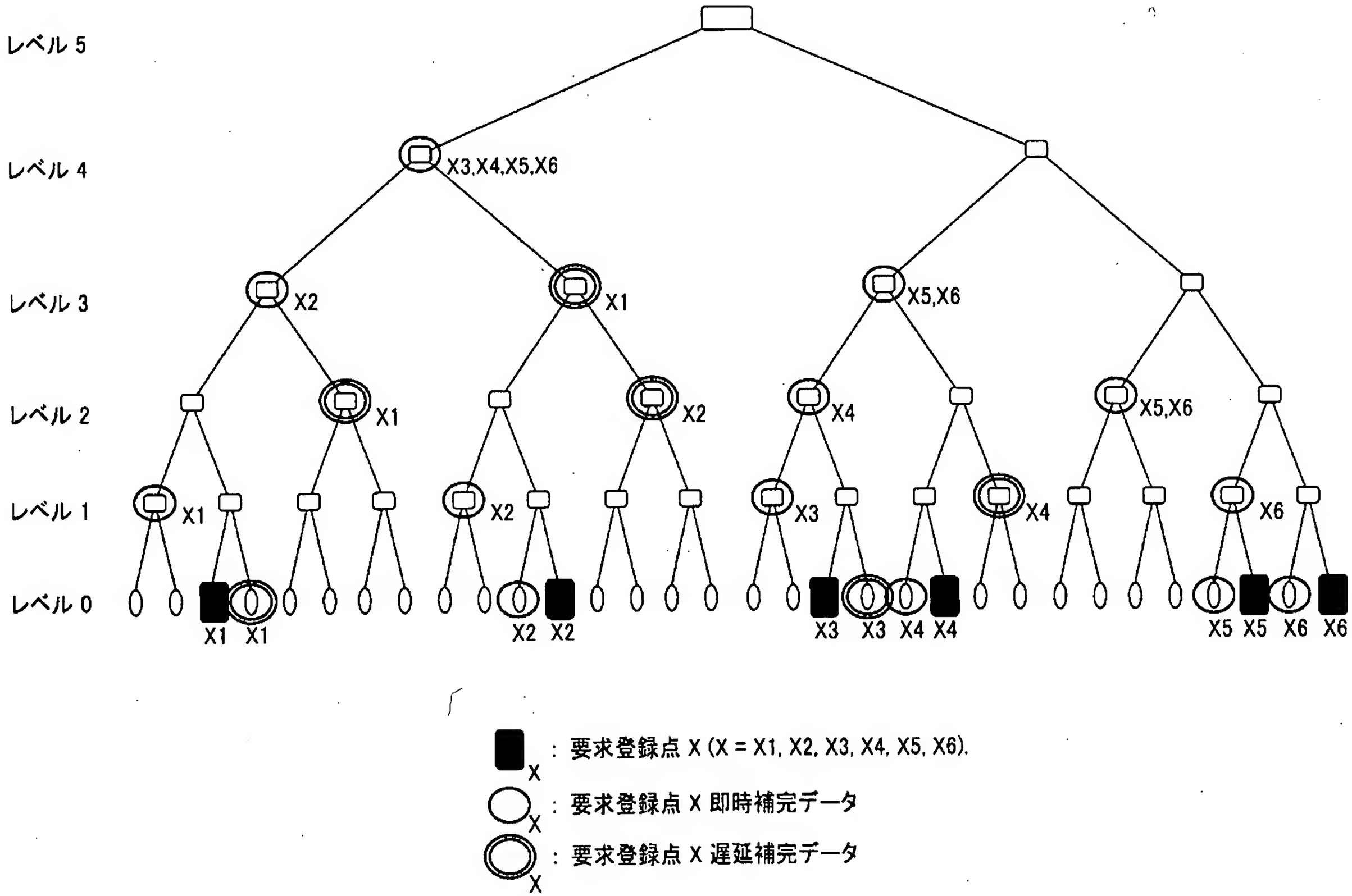

レベル0
レベル1
レベル2
レベル3
レベル4
V(0, 0)
V(0, 1)
V(0, 2)
V(0, 3)
V(0, 4)
V(0, 5)
V(0, 6)
V(0, 7)
V(0, 8)
V(0, 9)
V(0, 10)
V(0, 11)
V(0, 15)
V(1, 3)
V(1, 4)
V(2, 0)
V(3, 0)
V(3, 1)
V(4, 0)

【図３】

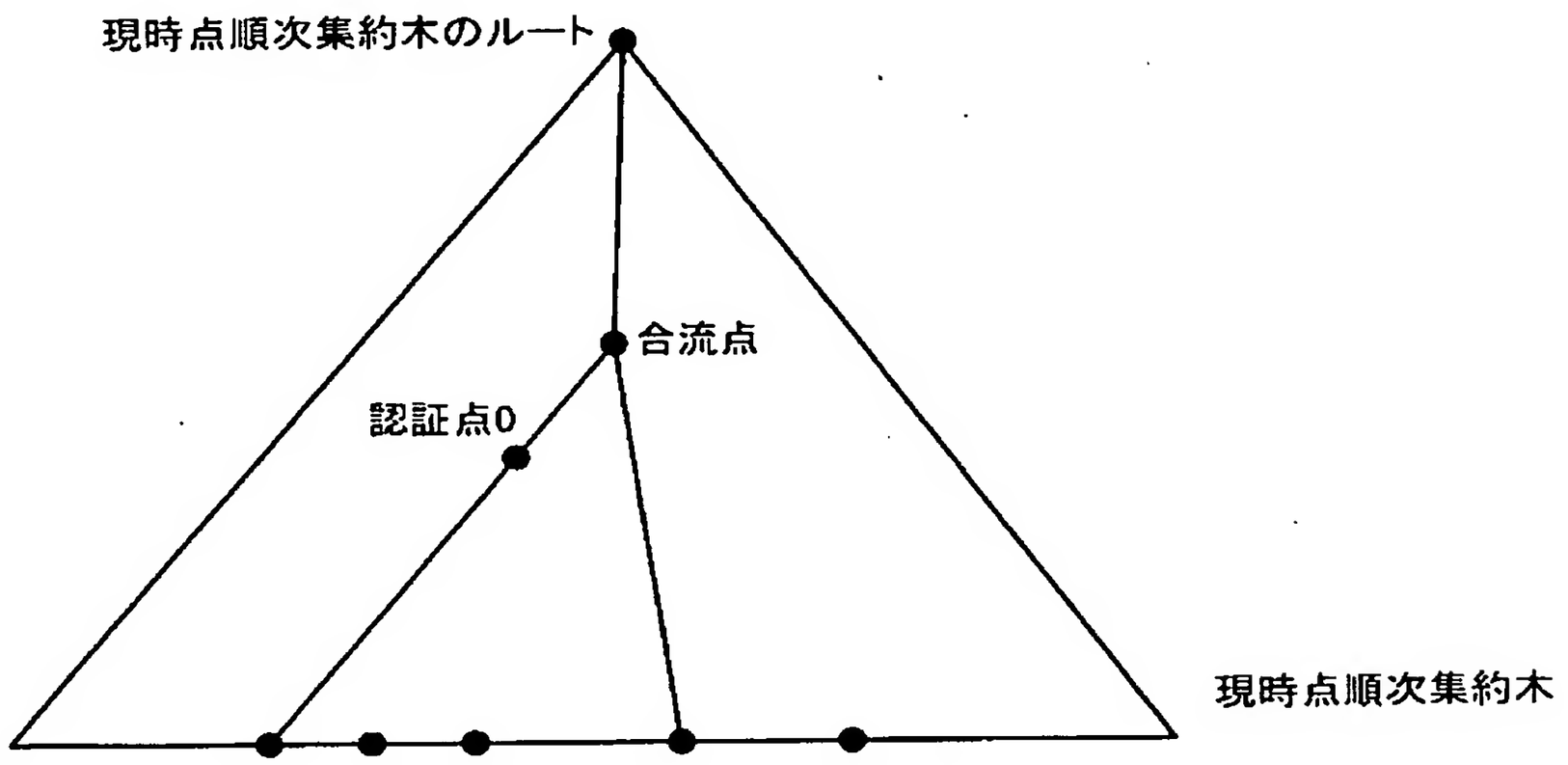
項目	記号	必須
元デジタルデータ	y	○
順次割当データ	z	○
順次集約木番号	n	○
順次集約木リーフ番号	i	○
登録点の即時補完データ(位置情報、割当値)	SK	○
過去の各登録点の遅延補完データ(位置情報、割当値)	TK	○

イベント順序受理証明書
EOC(y)

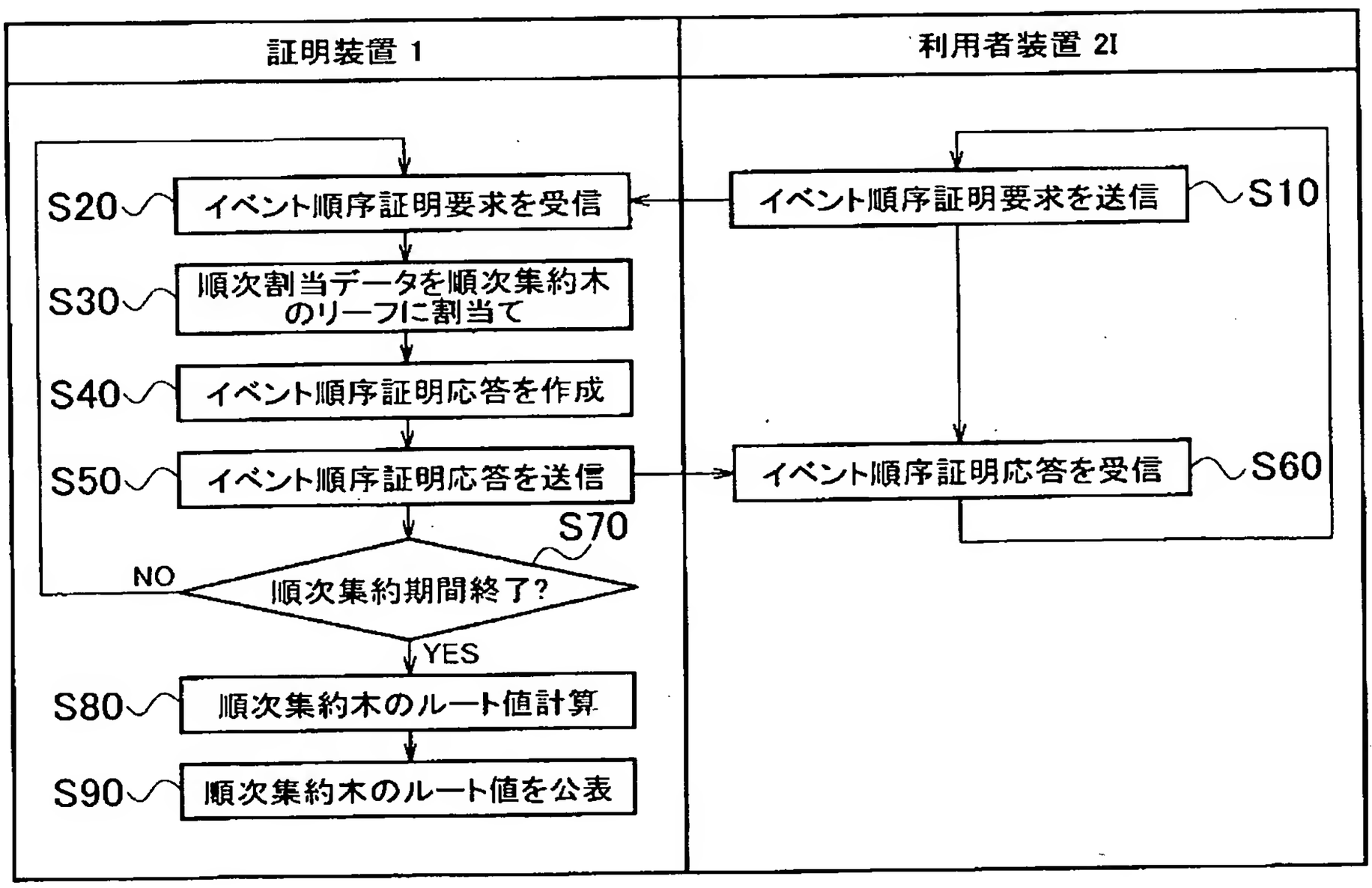
【図４】


レベル 5
レベル 4
レベル 3
レベル 2
レベル 1
レベル 0
X3,X4,X5,X6
X2
X1
X5,X6
X1
X2
X4
X5,X6
X1
X2
X3
X4
X6
X1 X1
X2 X2
X3 X3 X4 X4
X5 X5 X6 X6
X : 要求登録点 X (X = X1, X2, X3, X4, X5, X6).
X : 要求登録点 X 即時補完データ
X : 要求登録点 X 遅延補完データ

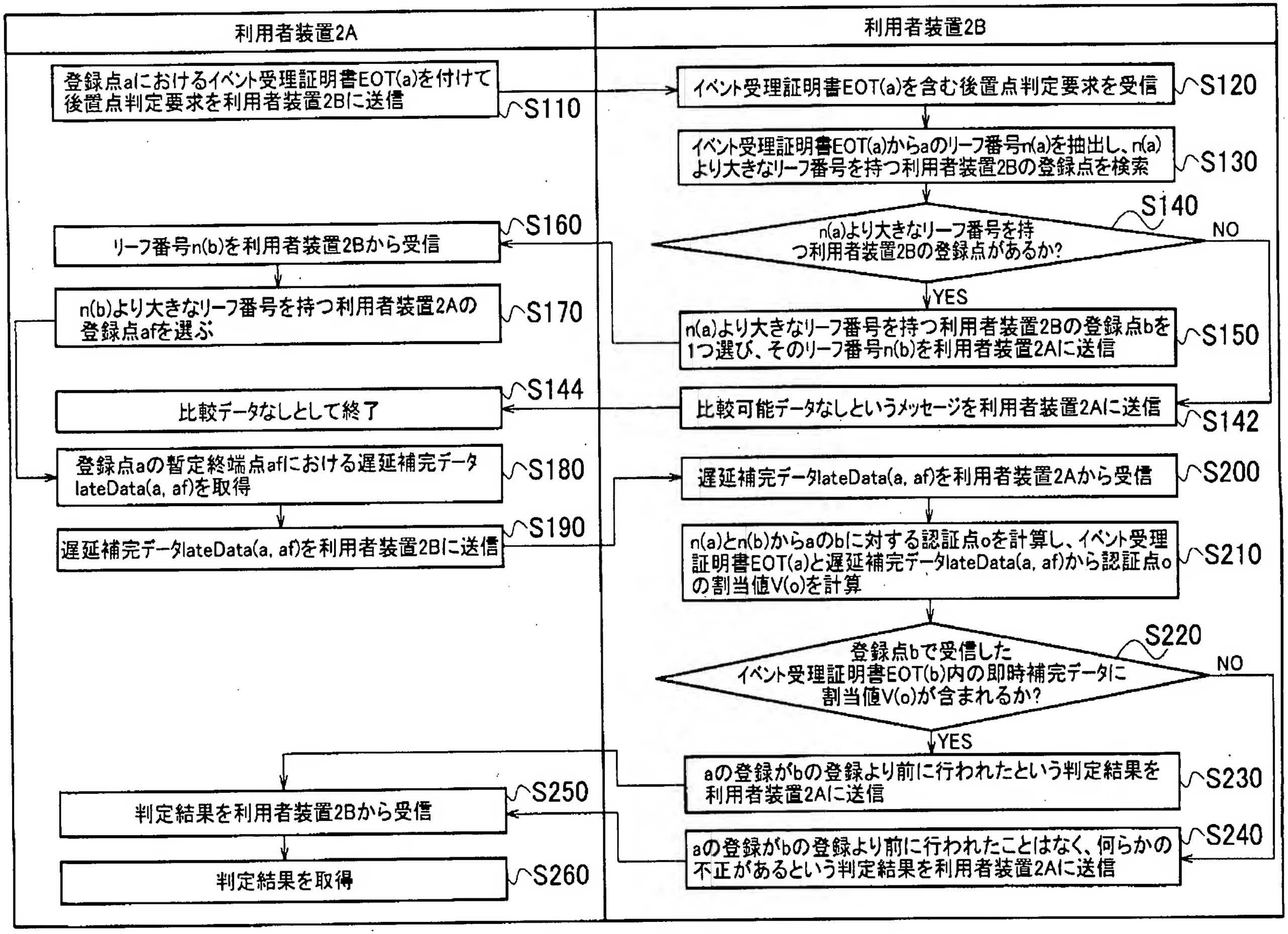
【図５】


現時点順次集約木のルート
合流点
認証点0
現時点順次集約木
a
a1
a2
b
af

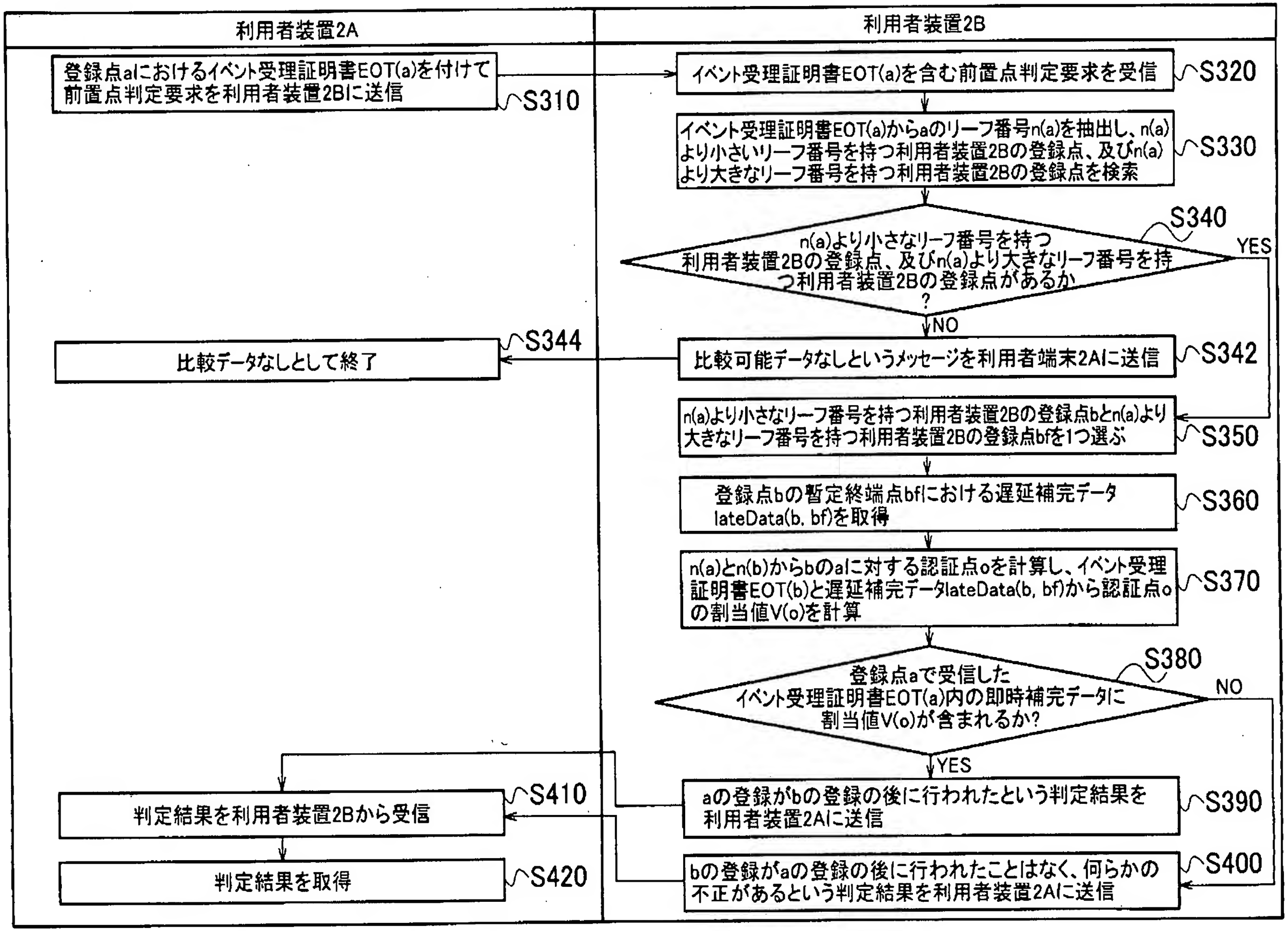
【図６】


証明装置 1
利用者装置 2I
S20
イベント順序証明要求を受信
S30
順次割当データを順次集約木のリーフに割当て
S40
イベント順序証明応答を作成
S50
イベント順序証明応答を送信
S70
順次集約期間終了?
NO
YES
S80
順次集約木のルート値計算
S90
順次集約木のルート値を公表
イベント順序証明要求を送信
S10
イベント順序証明応答を受信
S60

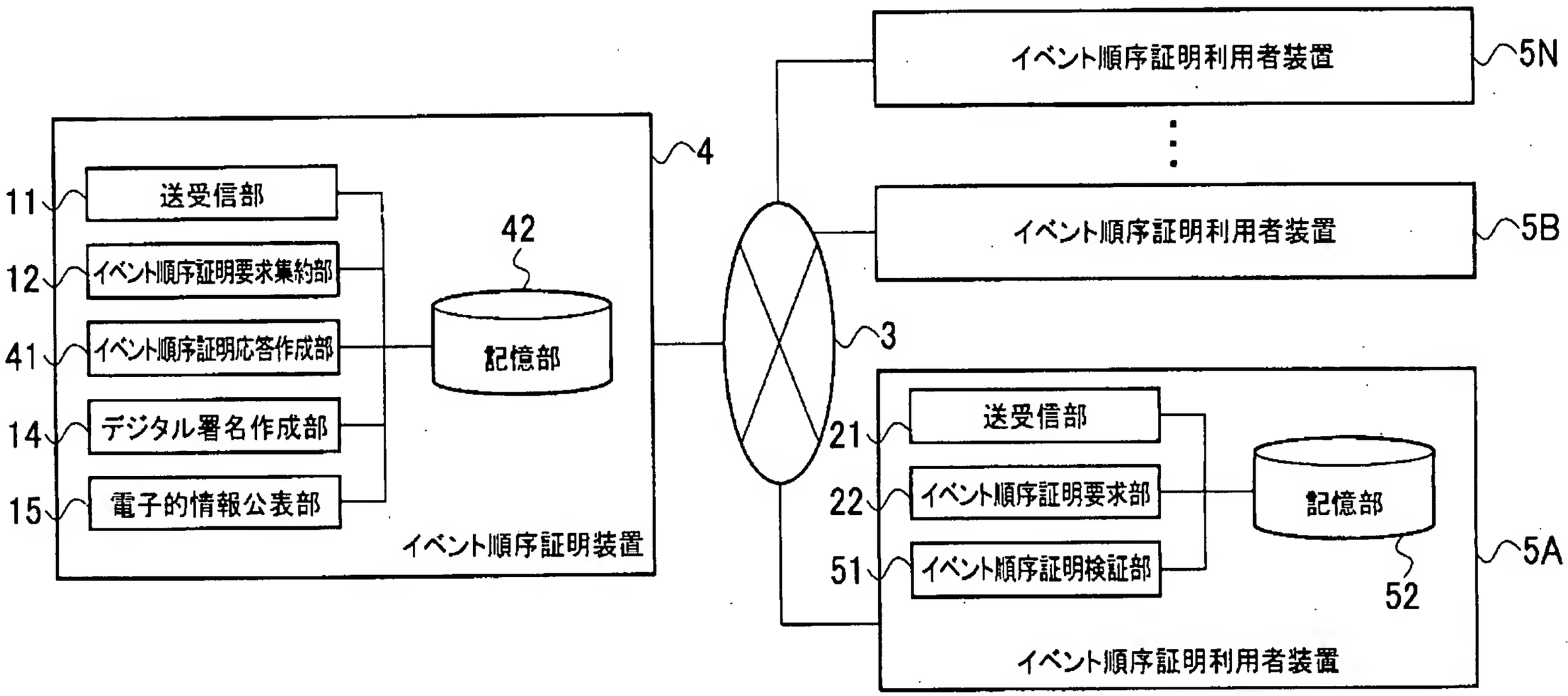
【図７】


利用者装置2A
利用者装置2B
登録点aにおけるイベント受理証明書EOT(a)を付けて後置点判定要求を利用者装置2Bに送信
S110
イベント受理証明書EOT(a)を含む後置点判定要求を受信
S120
イベント受理証明書EOT(a)からaのリーフ番号n(a)を抽出し、n(a)より大きなリーフ番号を持つ利用者装置2Bの登録点を検索
S130
n(a)より大きなリーフ番号を持つ利用者装置2Bの登録点があるか?
S140
NO
YES
n(a)より大きなリーフ番号を持つ利用者装置2Bの登録点bを1つ選び、そのリーフ番号n(b)を利用者装置2Aに送信
S150
比較可能データなしというメッセージを利用者装置2Aに送信
S142
リーフ番号n(b)を利用者装置2Bから受信
S160
n(b)より大きなリーフ番号を持つ利用者装置2Aの登録点afを選ぶ
S170
比較データなしとして終了
S144
登録点aの暫定終端点afにおける遅延補完データlateData(a, af)を取得
S180
遅延補完データlateData(a, af)を利用者装置2Bに送信
S190
遅延補完データlateData(a, af)を利用者装置2Aから受信
S200
n(a)とn(b)からaのbに対する認証点oを計算し、イベント受理証明書EOT(a)と遅延補完データlateData(a, af)から認証点oの割当値V(o)を計算
S210
登録点bで受信したイベント受理証明書EOT(b)内の即時補完データに割当値V(o)が含まれるか?
S220
NO
YES
aの登録がbの登録より前に行われたという判定結果を利用者装置2Aに送信
S230
aの登録がbの登録より前に行われたことはなく、何らかの不正があるという判定結果を利用者装置2Aに送信
S240
判定結果を利用者装置2Bから受信
S250
判定結果を取得
S260

【図８】


利用者装置2A
利用者装置2B
登録点aにおけるイベント受理証明書EOT(a)を付けて前置点判定要求を利用者装置2Bに送信
S310
イベント受理証明書EOT(a)を含む前置点判定要求を受信
S320
イベント受理証明書EOT(a)からaのリーフ番号n(a)を抽出し、n(a)より小さいリーフ番号を持つ利用者装置2Bの登録点、及びn(a)より大きなリーフ番号を持つ利用者装置2Bの登録点を検索
S330
n(a)より小さなリーフ番号を持つ利用者装置2Bの登録点、及びn(a)より大きなリーフ番号を持つ利用者装置2Bの登録点があるか？
S340
YES
NO
比較データなしとして終了
S344
比較可能データなしというメッセージを利用者端末2Aに送信
S342
n(a)より小さなリーフ番号を持つ利用者装置2Bの登録点bとn(a)より大きなリーフ番号を持つ利用者装置2Bの登録点bfを1つ選ぶ
S350
登録点bの暫定終端点bfにおける遅延補完データlateData(b, bf)を取得
S360
n(a)とn(b)からbのaに対する認証点oを計算し、イベント受理証明書EOT(b)と遅延補完データlateData(b, bf)から認証点oの割当値V(o)を計算
S370
登録点aで受信したイベント受理証明書EOT(a)内の即時補完データに割当値V(o)が含まれるか?
S380
NO
YES
判定結果を利用者装置2Bから受信
S410
aの登録がbの登録の後に行われたという判定結果を利用者装置2Aに送信
S390
判定結果を取得
S420
bの登録がaの登録の後に行われたことはなく、何らかの不正があるという判定結果を利用者装置2Aに送信
S400

【図９】

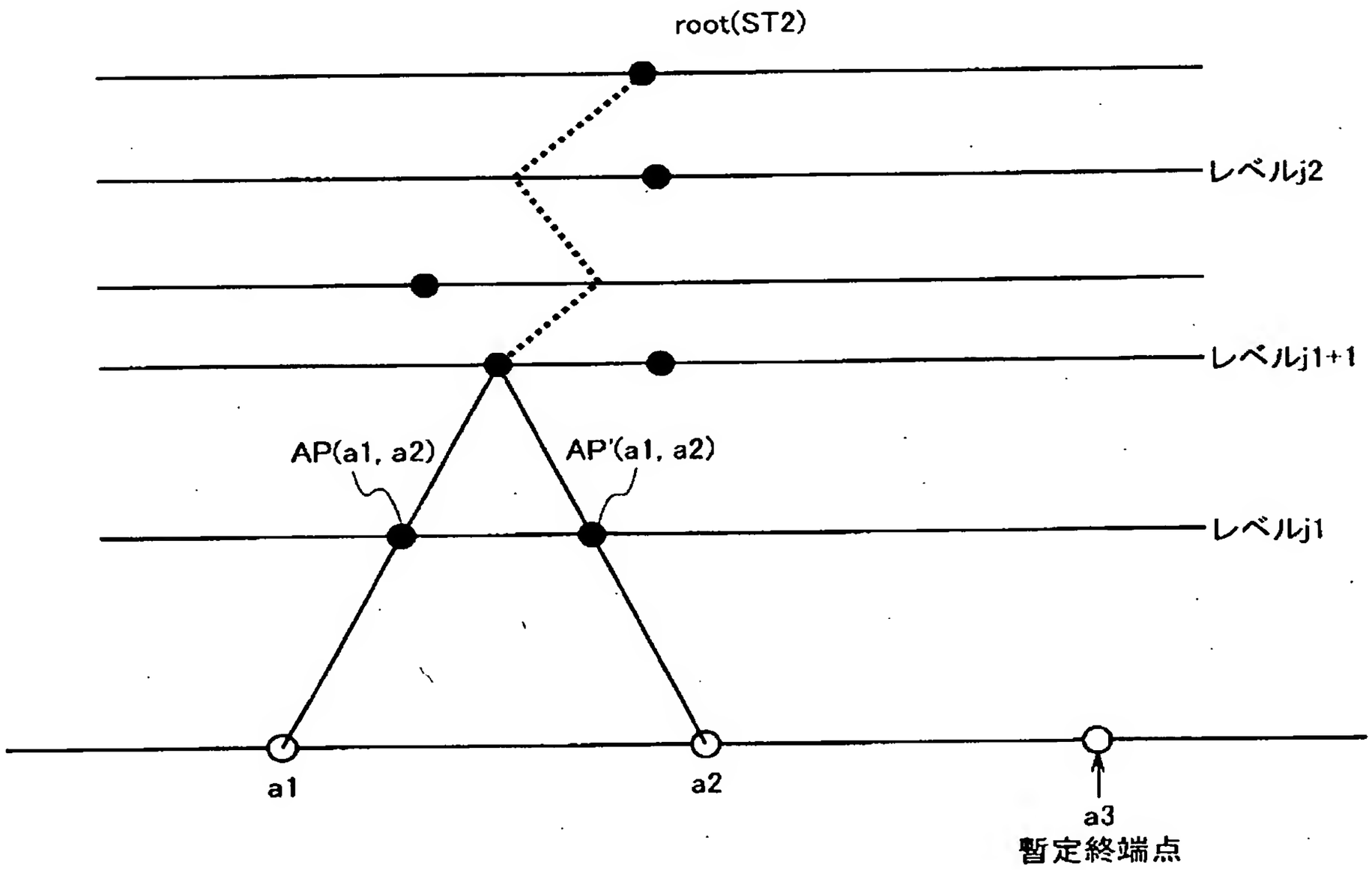

イベント順序証明利用者装置
5N
イベント順序証明利用者装置
5B
4
11
送受信部
12
イベント順序証明要求集約部
42
41
イベント順序証明応答作成部
記憶部
14
デジタル署名作成部
15
電子的情報公表部
イベント順序証明装置
3
21
送受信部
22
イベント順序証明要求部
記憶部
51
イベント順序証明検証部
52
5A
イベント順序証明利用者装置
200
イベント順序証明システム

【図１０】

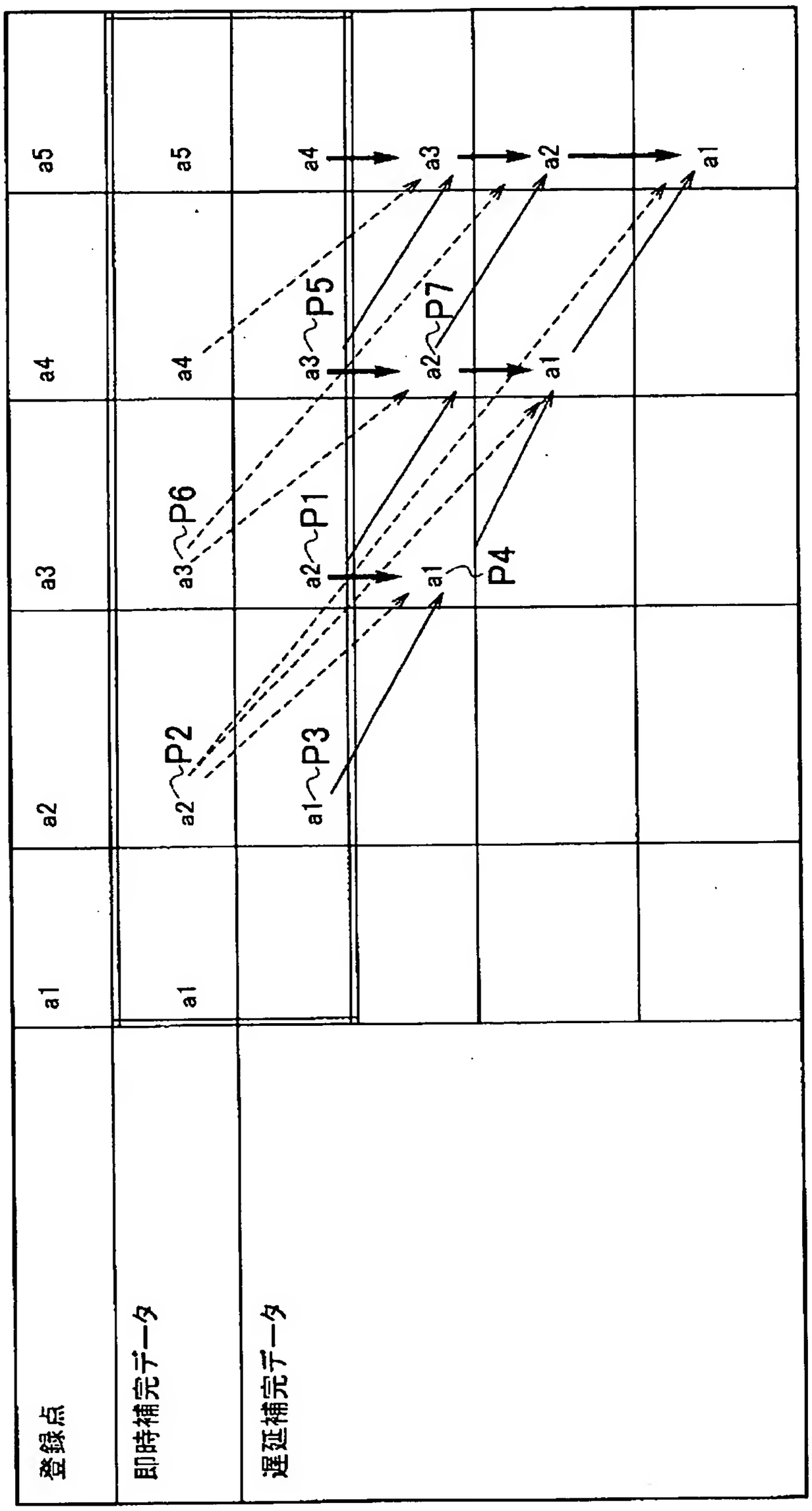
項目	記号	必須
元デジタルデータ	y	○
順次割当データ	z	○
順次集約木識別番号	n	○
順次集約木リーフ番号	i	○
登録点の即時補完データ(位置情報、割当値)	SK	○
直前登録点の遅延補完データ(位置情報、割当値)	TK2	○

イベント順序受理証明書
EOC(y)

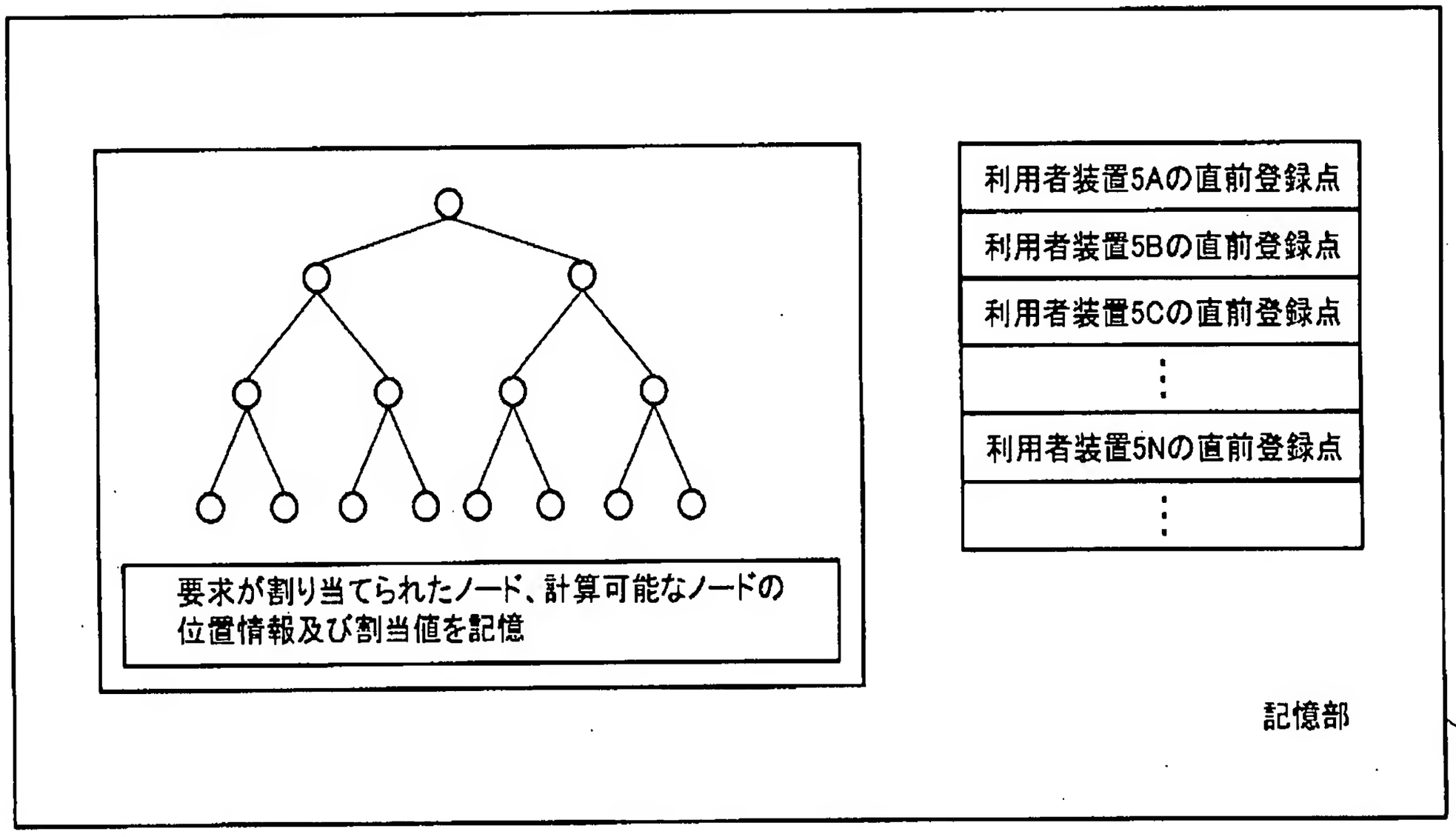
【図１１】



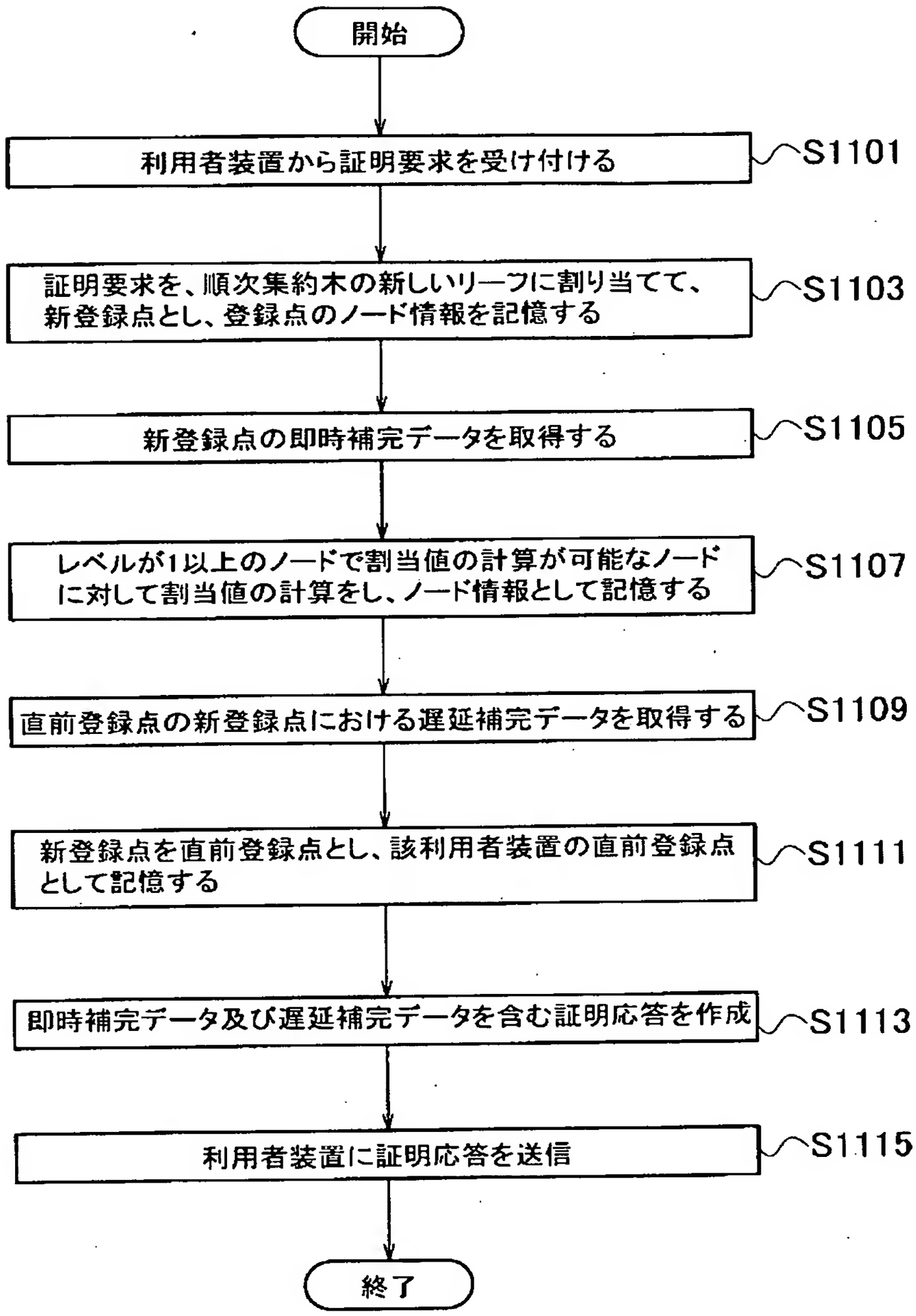
【図１２】


a5
a4
a3
a2
a1
a5
a4
a3
a2
a1
a4
a3
a2
a1
a3
a2
a1
a2
a1
a1
P1
P2
P3
P4
P5
P6
P7
登録点
即時補完データ
遅延補完データ

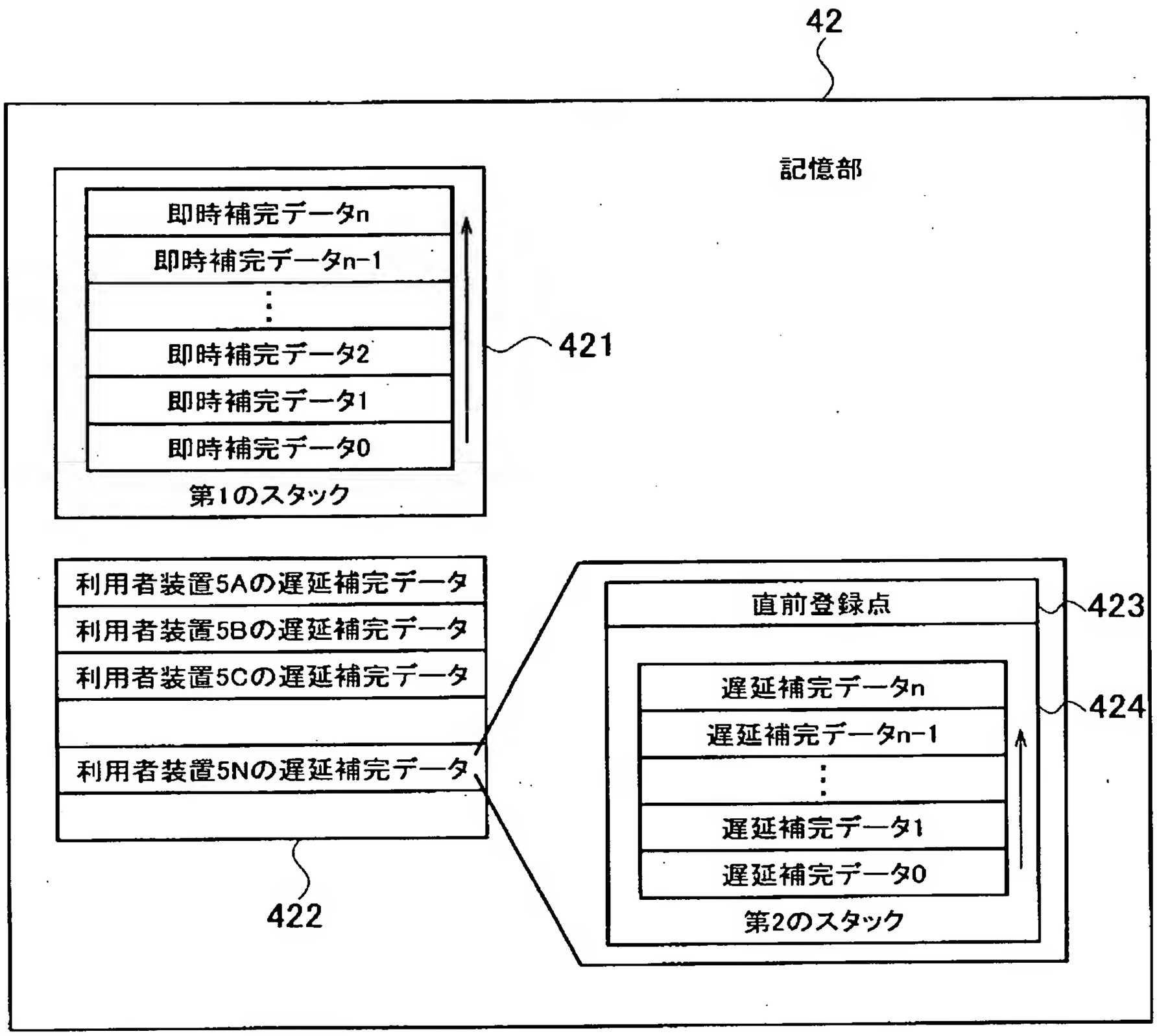
【図１３】


利用者装置5Aの直前登録点
利用者装置5Bの直前登録点
利用者装置5Cの直前登録点
利用者装置5Nの直前登録点
要求が割り当てられたノード、計算可能なノードの
位置情報及び割当値を記憶
記憶部
42

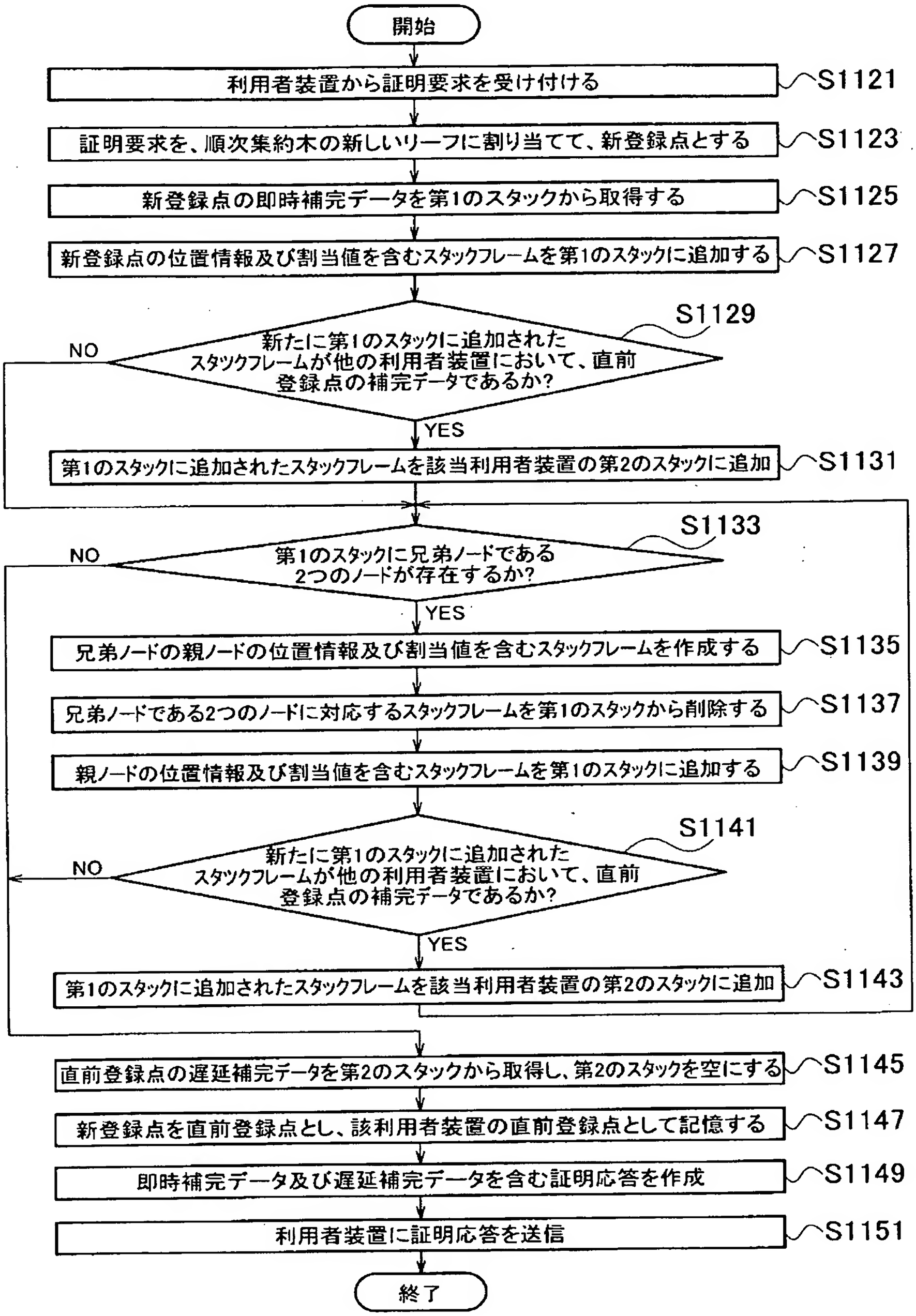
【図１４】


開始
利用者装置から証明要求を受け付ける
S1101
証明要求を、順次集約木の新しいリーフに割り当てて、新登録点とし、登録点のノード情報を記憶する
S1103
新登録点の即時補完データを取得する
S1105
レベルが1以上のノードで割当値の計算が可能なノードに対して割当値の計算をし、ノード情報として記憶する
S1107
直前登録点の新登録点における遅延補完データを取得する
S1109
新登録点を直前登録点とし、該利用者装置の直前登録点として記憶する
S1111
即時補完データ及び遅延補完データを含む証明応答を作成
S1113
利用者装置に証明応答を送信
S1115
終了

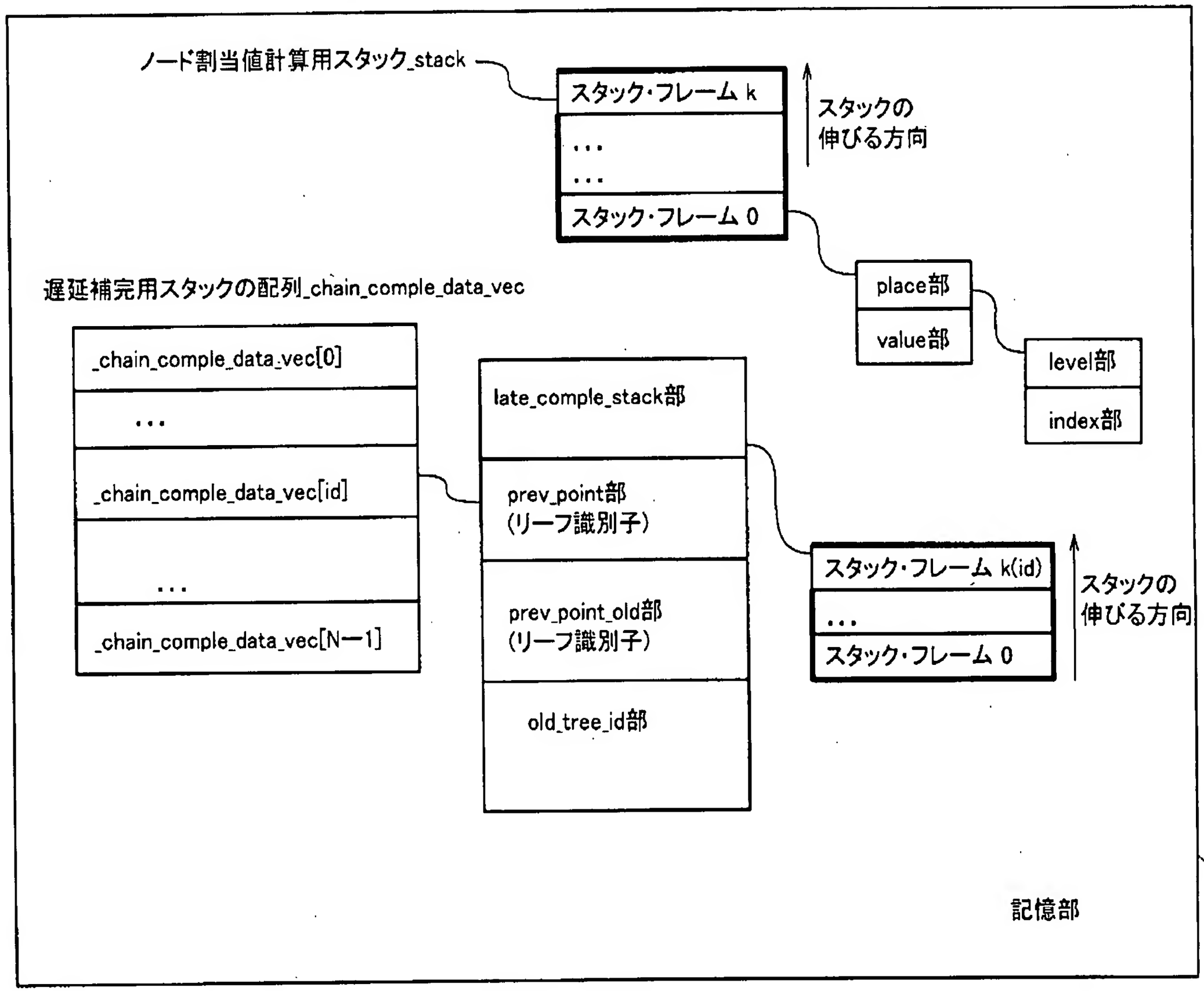
【図１５】


42
記憶部
即時補完データn
即時補完データn-1
即時補完データ2
即時補完データ1
即時補完データ0
第1のスタック
421
利用者装置5Aの遅延補完データ
利用者装置5Bの遅延補完データ
利用者装置5Cの遅延補完データ
利用者装置5Nの遅延補完データ
422
直前登録点
423
遅延補完データn
遅延補完データn-1
遅延補完データ1
遅延補完データ0
第2のスタック
424

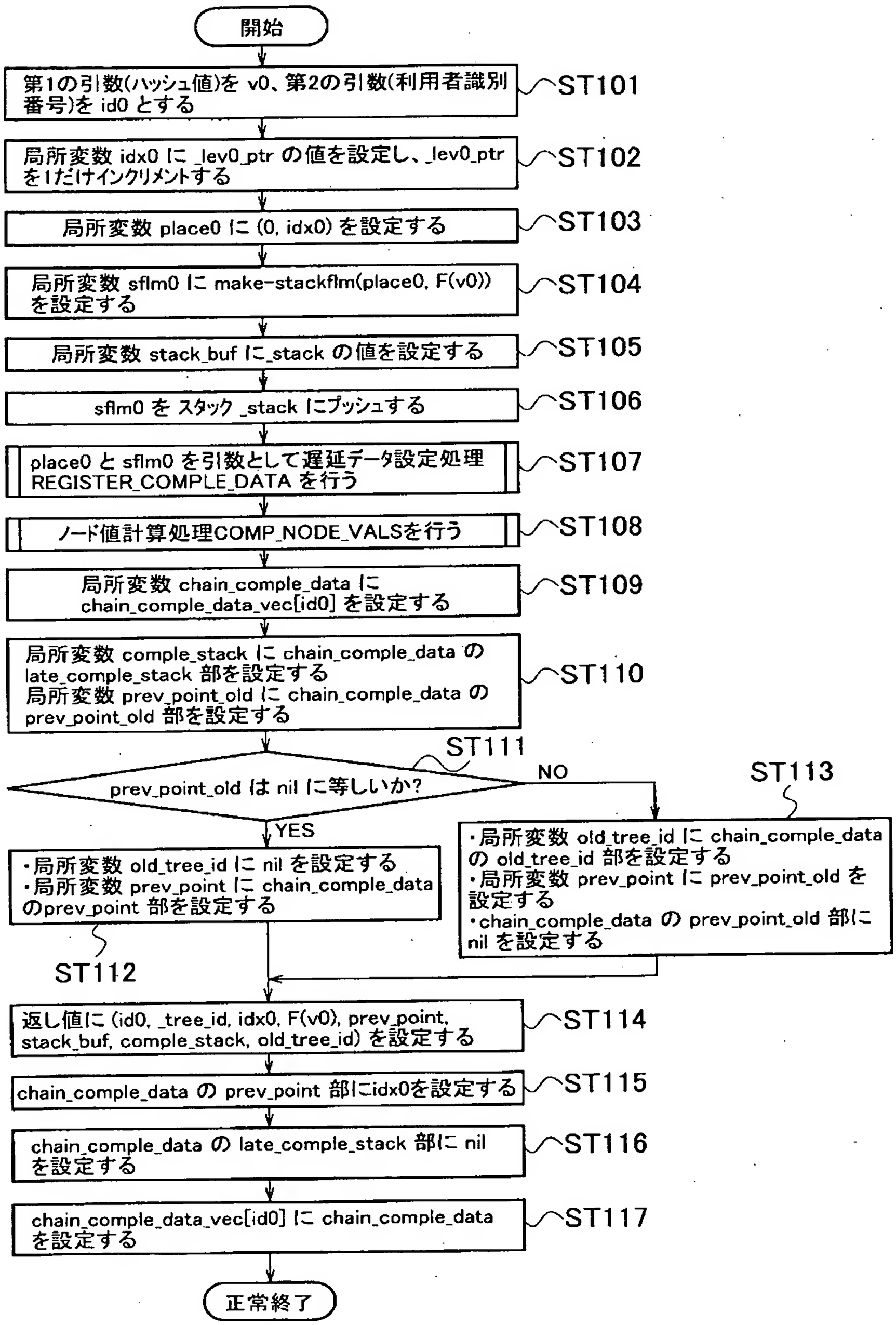
【図１６】


開始
利用者装置から証明要求を受け付ける
S1121
証明要求を、順次集約木の新しいリーフに割り当てて、新登録点とする
S1123
新登録点の即時補完データを第1のスタックから取得する
S1125
新登録点の位置情報及び割当値を含むスタックフレームを第1のスタックに追加する
S1127
S1129
新たに第1のスタックに追加された
スタックフレームが他の利用者装置において、直前
登録点の補完データであるか?
NO
YES
第1のスタックに追加されたスタックフレームを該当利用者装置の第2のスタックに追加
S1131
S1133
第1のスタックに兄弟ノードである
2つのノードが存在するか?
NO
YES
兄弟ノードの親ノードの位置情報及び割当値を含むスタックフレームを作成する
S1135
兄弟ノードである2つのノードに対応するスタックフレームを第1のスタックから削除する
S1137
親ノードの位置情報及び割当値を含むスタックフレームを第1のスタックに追加する
S1139
S1141
新たに第1のスタックに追加された
スタックフレームが他の利用者装置において、直前
登録点の補完データであるか?
NO
YES
第1のスタックに追加されたスタックフレームを該当利用者装置の第2のスタックに追加
S1143
直前登録点の遅延補完データを第2のスタックから取得し、第2のスタックを空にする
S1145
新登録点を直前登録点とし、該利用者装置の直前登録点として記憶する
S1147
即時補完データ及び遅延補完データを含む証明応答を作成
S1149
利用者装置に証明応答を送信
S1151
終了

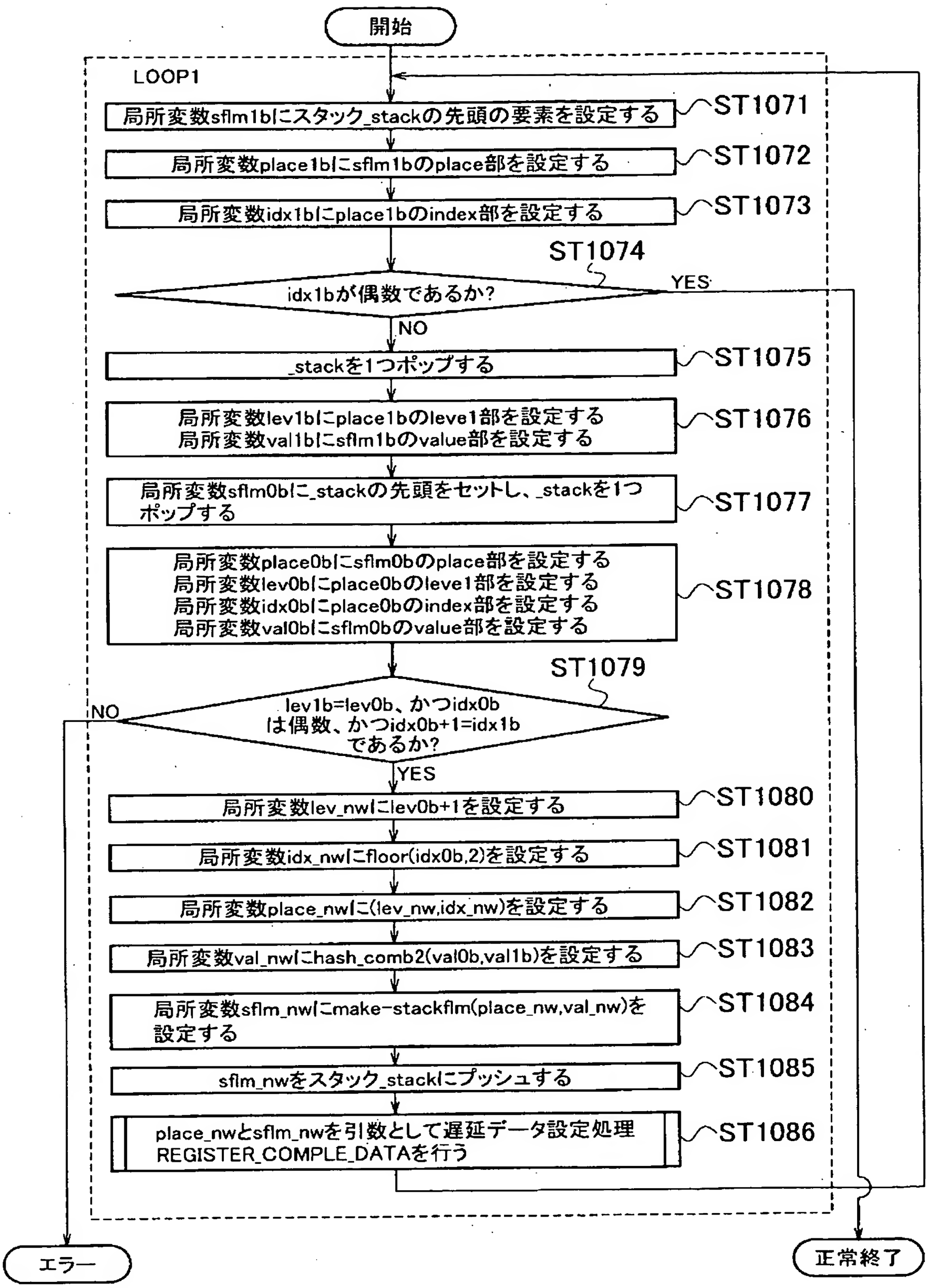
【図17】


ノード割当値計算用スタック_stack
スタック・フレーム k
...
...
スタック・フレーム 0
スタックの
伸びる方向
place部
value部
level部
index部
遅延補完用スタックの配列_chain_comple_data_vec
_chain_comple_data_vec[0]
...
_chain_comple_data_vec[id]
...
_chain_comple_data_vec[N−1]
late_comple_stack部
prev_point部
(リーフ識別子)
prev_point_old部
(リーフ識別子)
old_tree_id部
スタック・フレーム k(id)
...
スタック・フレーム 0
スタックの
伸びる方向
42
記憶部

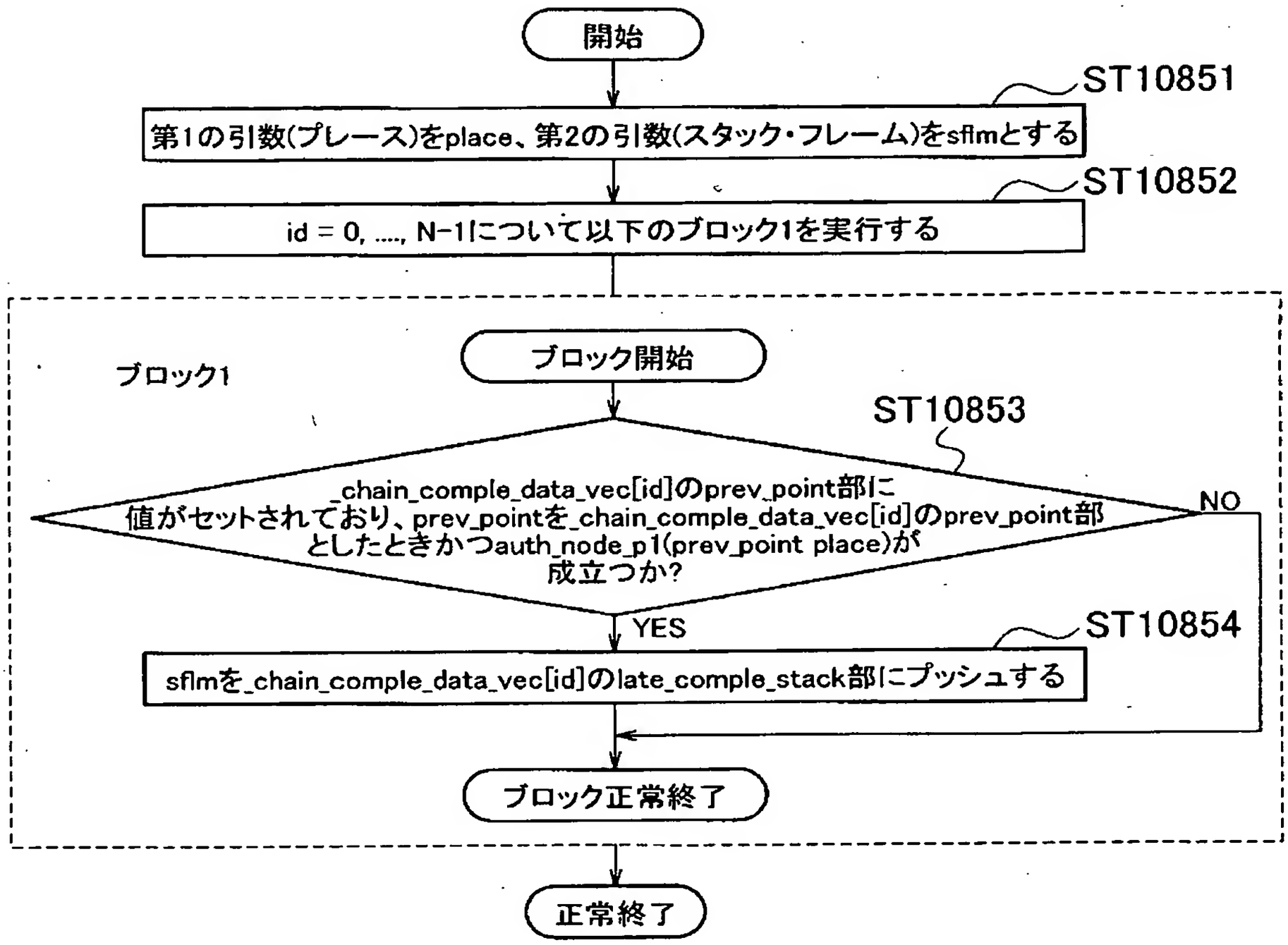
【図１８】


開始
第1の引数(ハッシュ値)を v0、第2の引数(利用者識別番号)を id0 とする
ST101
局所変数 idx0 に _lev0_ptr の値を設定し、_lev0_ptr を1だけインクリメントする
ST102
局所変数 place0 に (0, idx0) を設定する
ST103
局所変数 sflm0 に make-stackflm(place0, F(v0)) を設定する
ST104
局所変数 stack_buf に_stack の値を設定する
ST105
sflm0 を スタック _stack にプッシュする
ST106
place0 と sflm0 を引数として遅延データ設定処理 REGISTER_COMPLE_DATA を行う
ST107
ノード値計算処理COMP_NODE_VALSを行う
ST108
局所変数 chain_comple_data に chain_comple_data_vec[id0] を設定する
ST109
局所変数 comple_stack に chain_comple_data の late_comple_stack 部を設定する
局所変数 prev_point_old に chain_comple_data の prev_point_old 部を設定する
ST110
ST111
prev_point_old は nil に等しいか?
NO
YES
ST113
・局所変数 old_tree_id に chain_comple_data の old_tree_id 部を設定する
・局所変数 prev_point に prev_point_old を設定する
・chain_comple_data の prev_point_old 部に nil を設定する
・局所変数 old_tree_id に nil を設定する
・局所変数 prev_point に chain_comple_data のprev_point 部を設定する
ST112
返し値に (id0, _tree_id, idx0, F(v0), prev_point, stack_buf, comple_stack, old_tree_id) を設定する
ST114
chain_comple_data の prev_point 部にidx0を設定する
ST115
chain_comple_data の late_comple_stack 部に nil を設定する
ST116
chain_comple_data_vec[id0] に chain_comple_data を設定する
ST117
正常終了

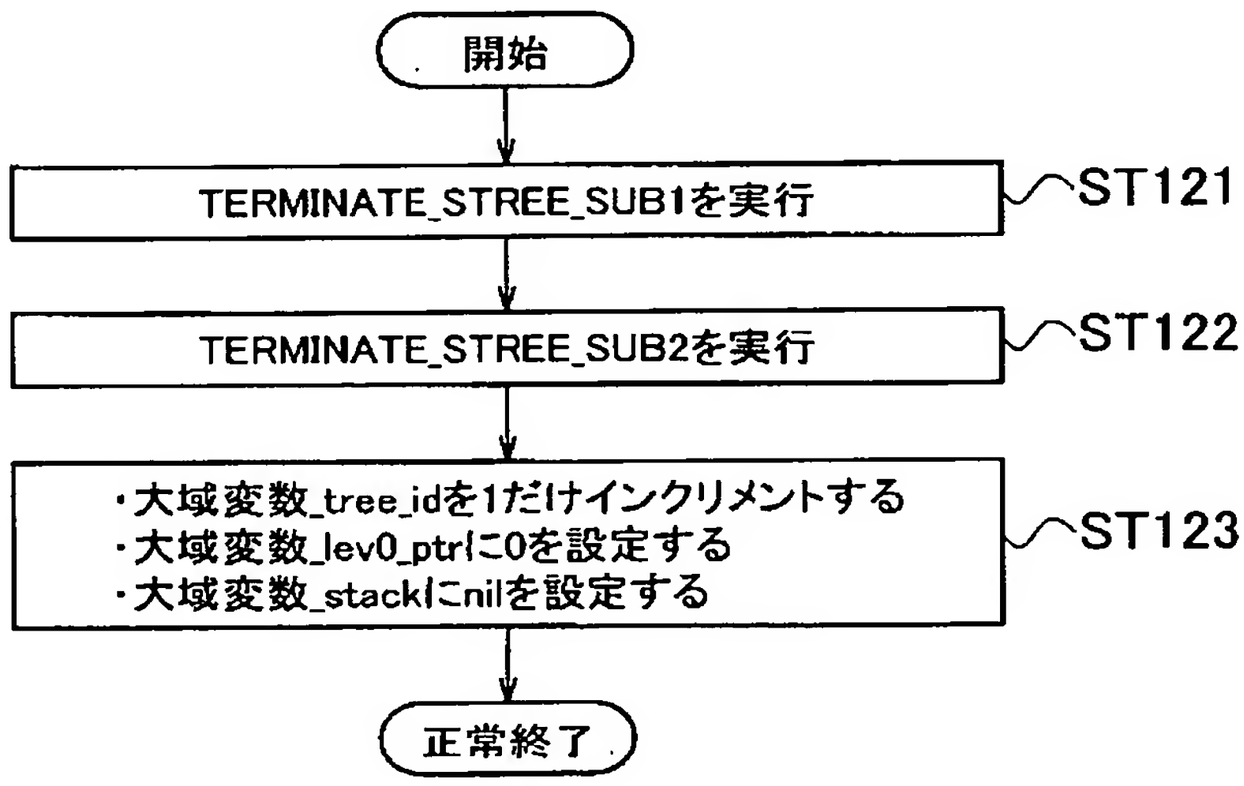
【図１９】


開始
LOOP1
局所変数sflm1bにスタック_stackの先頭の要素を設定する
ST1071
局所変数place1bにsflm1bのplace部を設定する
ST1072
局所変数idx1bにplace1bのindex部を設定する
ST1073
ST1074
idx1bが偶数であるか?
YES
NO
_stackを1つポップする
ST1075
局所変数lev1bにplace1bのleve1部を設定する
局所変数val1bにsflm1bのvalue部を設定する
ST1076
局所変数sflm0bに_stackの先頭をセットし、_stackを1つポップする
ST1077
局所変数place0bにsflm0bのplace部を設定する
局所変数lev0bにplace0bのleve1部を設定する
局所変数idx0bにplace0bのindex部を設定する
局所変数val0bにsflm0bのvalue部を設定する
ST1078
ST1079
lev1b=lev0b、かつidx0b
は偶数、かつidx0b+1=idx1b
であるか?
NO
YES
局所変数lev_nwにlev0b+1を設定する
ST1080
局所変数idx_nwにfloor(idx0b,2)を設定する
ST1081
局所変数place_nwに(lev_nw,idx_nw)を設定する
ST1082
局所変数val_nwにhash_comb2(val0b,val1b)を設定する
ST1083
局所変数sflm_nwにmake-stackflm(place_nw,val_nw)を設定する
ST1084
sflm_nwをスタック_stackにプッシュする
ST1085
place_nwとsflm_nwを引数として遅延データ設定処理REGISTER_COMPLE_DATAを行う
ST1086
エラー
正常終了

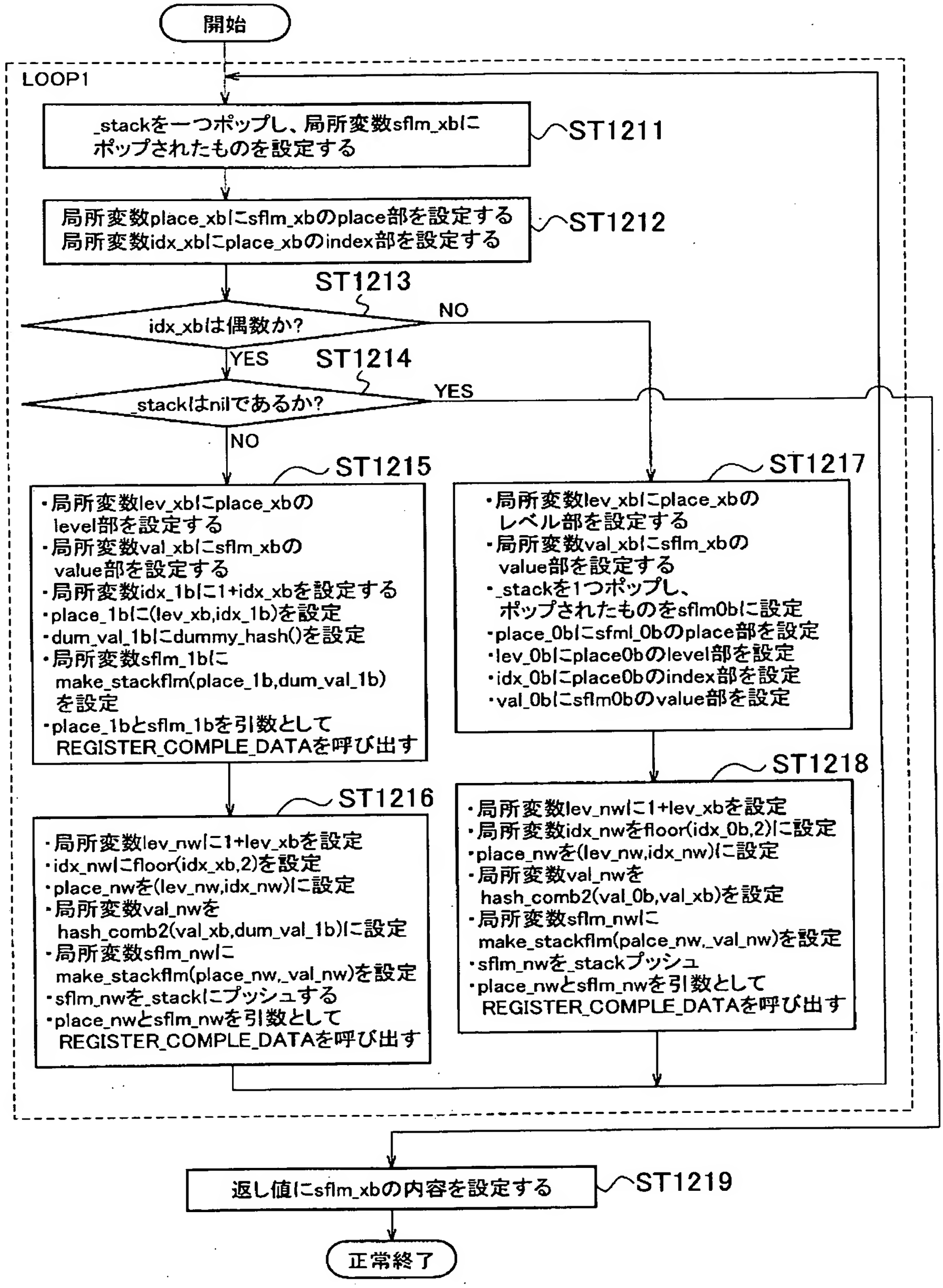
【図２０】


開始
ST10851
第1の引数(プレース)をplace、第2の引数(スタック・フレーム)をsflmとする
ST10852
id = 0, ..., N-1について以下のブロック1を実行する
ブロック1
ブロック開始
ST10853
_chain_comple_data_vec[id]のprev_point部に
値がセットされており、prev_pointを_chain_comple_data_vec[id]のprev_point部
としたときかつauth_node_p1(prev_point place)が
成立つか?
NO
YES
ST10854
sflmを_chain_comple_data_vec[id]のlate_comple_stack部にプッシュする
ブロック正常終了
正常終了

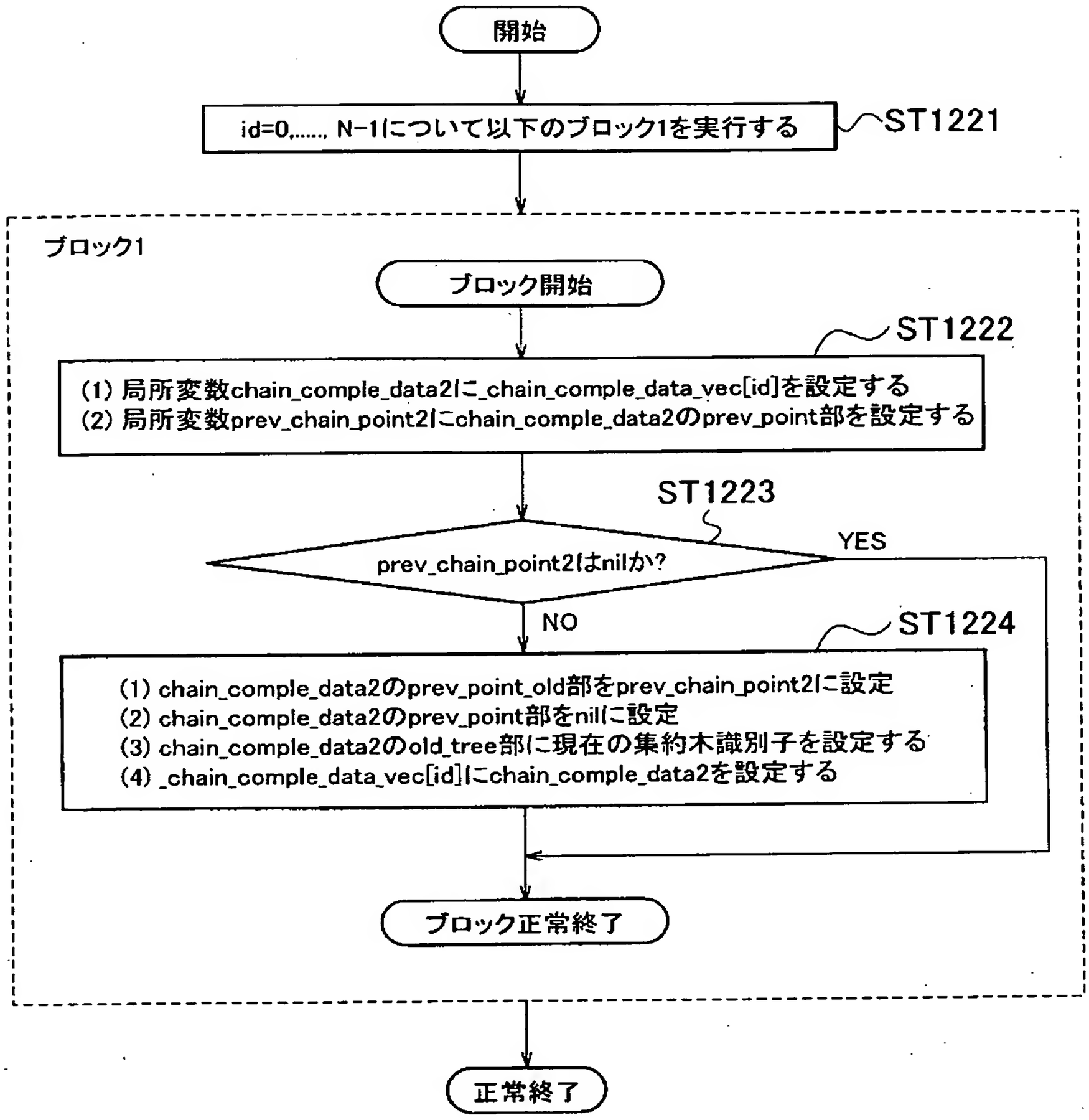
【図２１】


開始
TERMINATE_STREE_SUB1を実行
ST121
TERMINATE_STREE_SUB2を実行
ST122
・大域変数_tree_idを1だけインクリメントする
・大域変数_lev0_ptrに0を設定する
・大域変数_stackにnilを設定する
ST123
正常終了

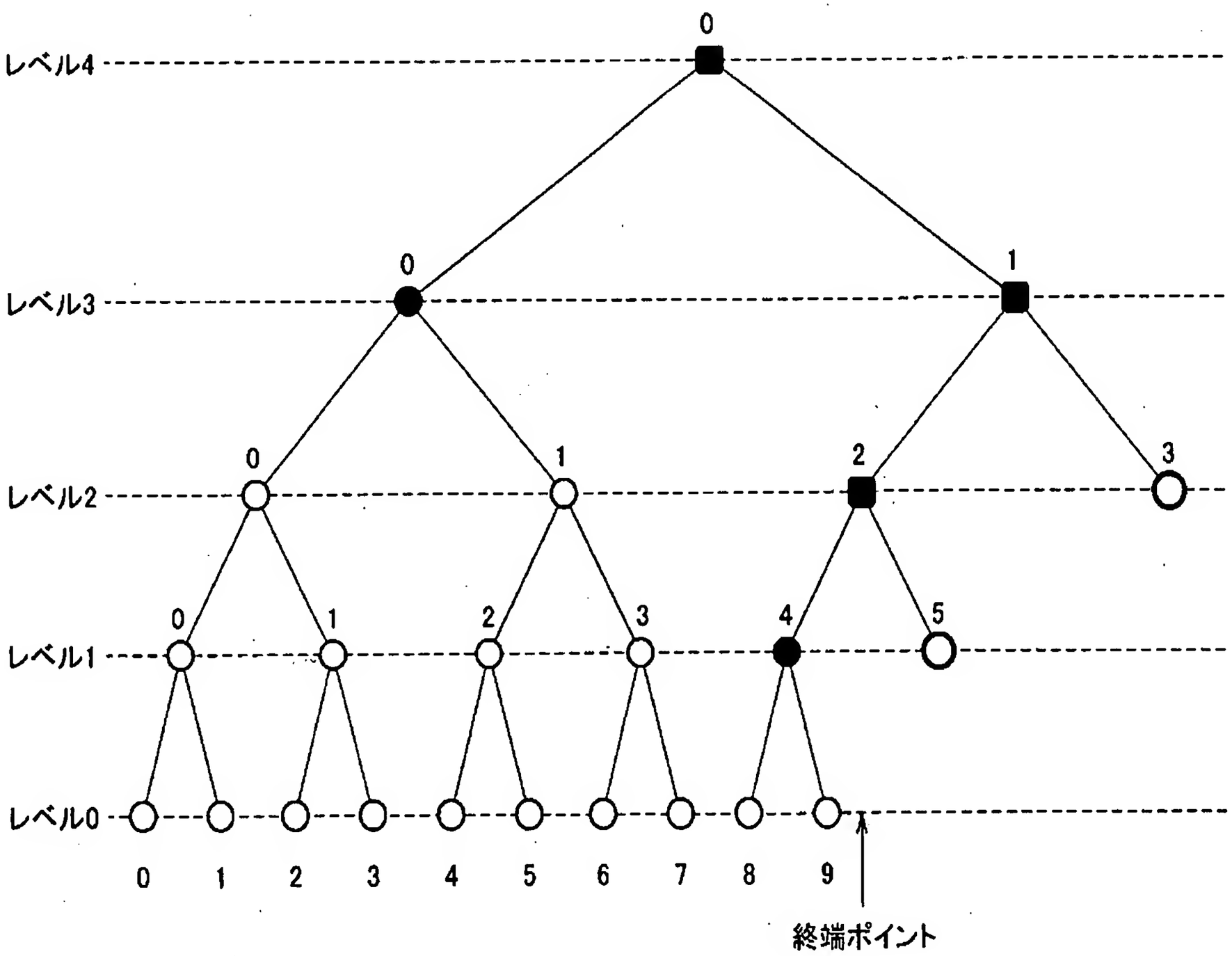
【図２２】

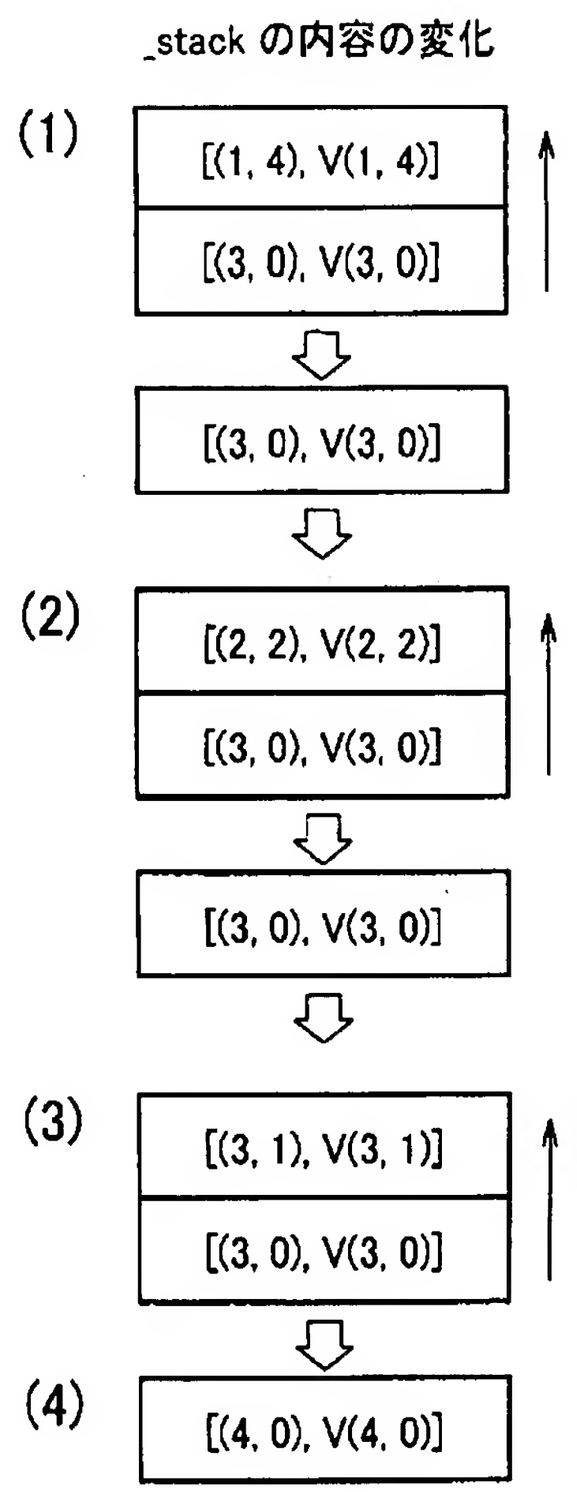

開始
LOOP1
_stackを一つポップし、局所変数sflm_xbに
ポップされたものを設定する
ST1211
局所変数place_xbにsflm_xbのplace部を設定する
局所変数idx_xbにplace_xbのindex部を設定する
ST1212
ST1213
idx_xbは偶数か?
NO
YES
ST1214
_stackはnilであるか?
YES
NO
ST1215
・局所変数lev_xbにplace_xbの
level部を設定する
・局所変数val_xbにsflm_xbの
value部を設定する
・局所変数idx_1bに1+idx_xbを設定する
・place_1bに(lev_xb,idx_1b)を設定
・dum_val_1bにdummy_hash()を設定
・局所変数sflm_1bに
make_stackflm(place_1b,dum_val_1b)
を設定
・place_1bとsflm_1bを引数として
REGISTER_COMPLE_DATAを呼び出す
ST1216
・局所変数lev_nwに1+lev_xbを設定
・idx_nwにfloor(idx_xb,2)を設定
・place_nwを(lev_nw,idx_nw)に設定
・局所変数val_nwを
hash_comb2(val_xb,dum_val_1b)に設定
・局所変数sflm_nwに
make_stackflm(place_nw,_val_nw)を設定
・sflm_nwを_stackにプッシュする
・place_nwとsflm_nwを引数として
REGISTER_COMPLE_DATAを呼び出す
ST1217
・局所変数lev_xbにplace_xbの
レベル部を設定する
・局所変数val_xbにsflm_xbの
value部を設定する
・_stackを1つポップし、
ポップされたものをsflm0bに設定
・place_0bにsfml_0bのplace部を設定
・lev_0bにplace0bのlevel部を設定
・idx_0bにplace0bのindex部を設定
・val_0bにsflm0bのvalue部を設定
ST1218
・局所変数lev_nwに1+lev_xbを設定
・局所変数idx_nwをfloor(idx_0b,2)に設定
・place_nwを(lev_nw,idx_nw)に設定
・局所変数val_nwを
hash_comb2(val_0b,val_xb)を設定
・局所変数sflm_nwに
make_stackflm(palce_nw,_val_nw)を設定
・sflm_nwを_stackプッシュ
・place_nwとsflm_nwを引数として
REGISTER_COMPLE_DATAを呼び出す
返し値にsflm_xbの内容を設定する
ST1219
正常終了

【図２３】

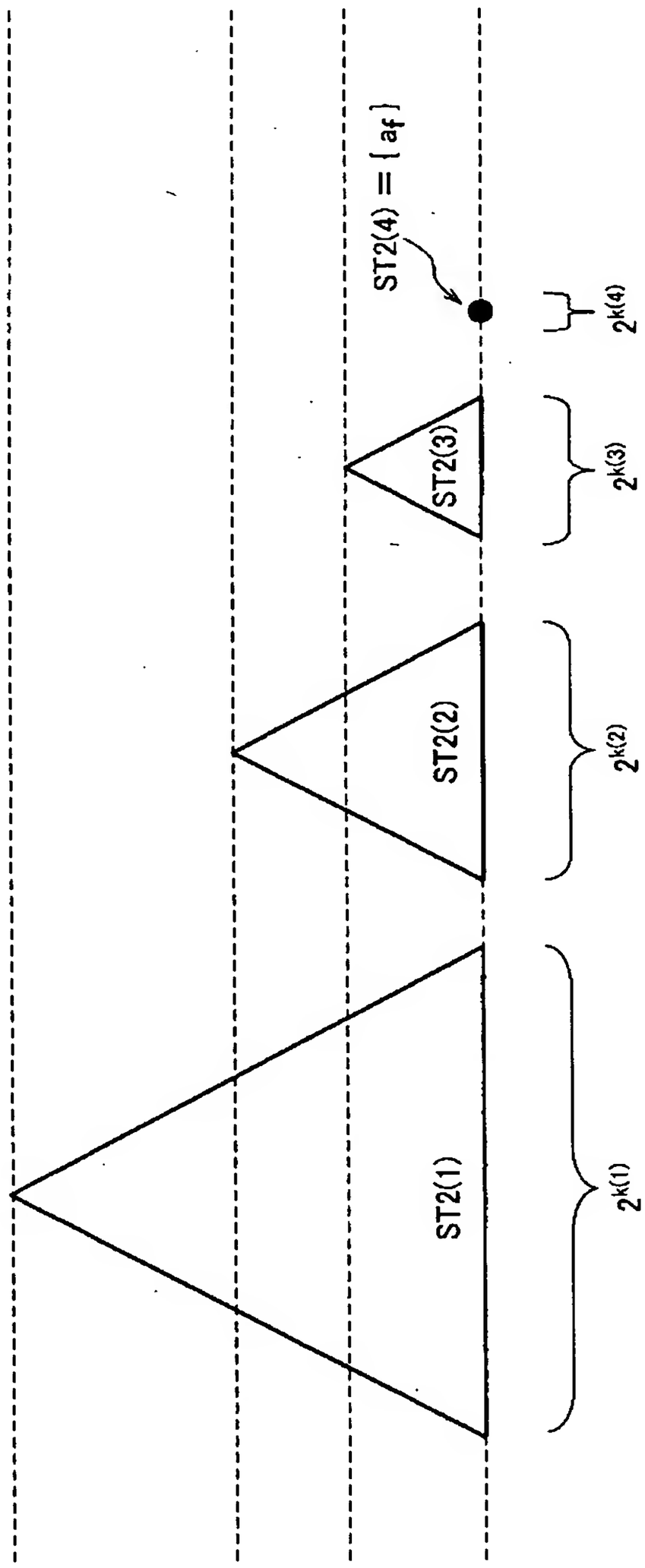

開始
id=0,....., N-1について以下のブロック1を実行する
ST1221
ブロック1
ブロック開始
ST1222
(1) 局所変数chain_comple_data2に_chain_comple_data_vec[id]を設定する
(2) 局所変数prev_chain_point2にchain_comple_data2のprev_point部を設定する
ST1223
prev_chain_point2はnilか?
YES
NO
ST1224
(1) chain_comple_data2のprev_point_old部をprev_chain_point2に設定
(2) chain_comple_data2のprev_point部をnilに設定
(3) chain_comple_data2のold_tree部に現在の集約木識別子を設定する
(4) _chain_comple_data_vec[id]にchain_comple_data2を設定する
ブロック正常終了
正常終了

【図２４】

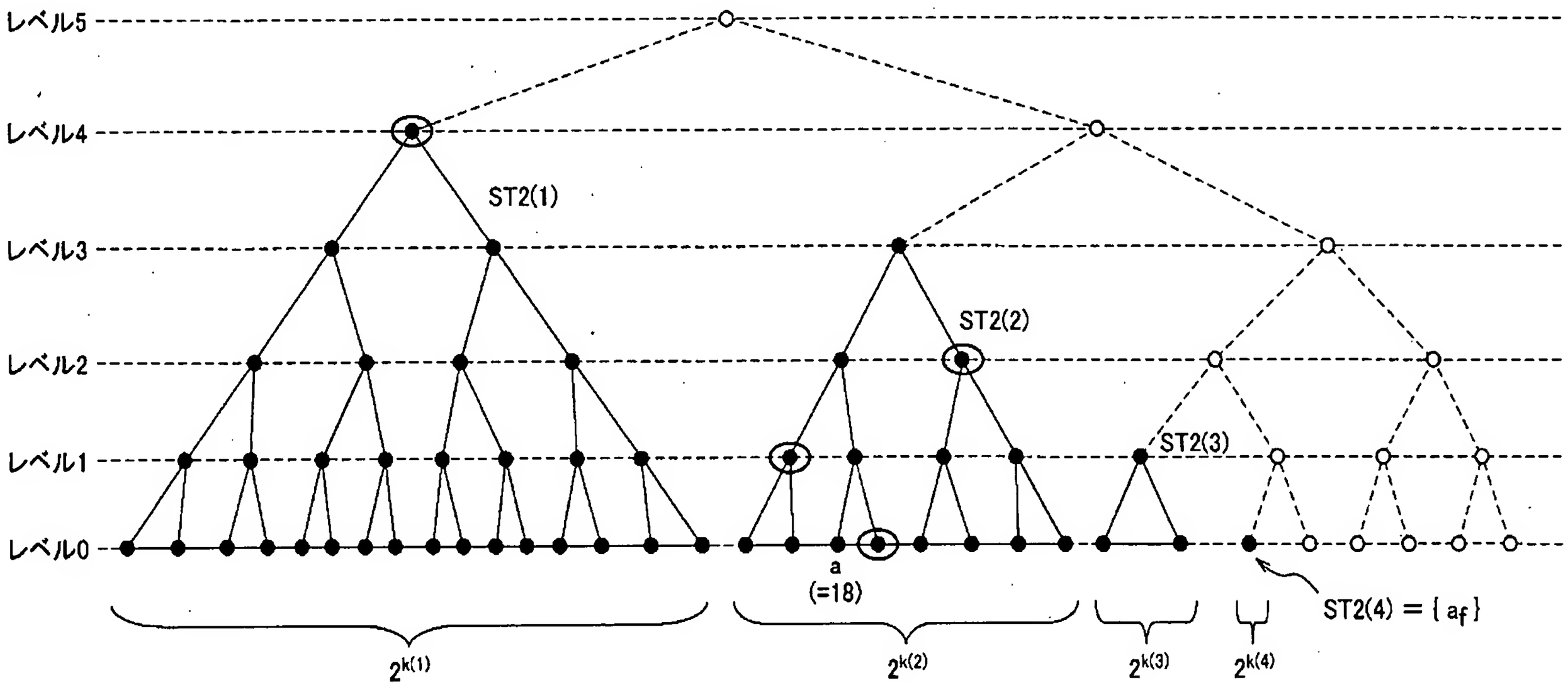

レベル4
レベル3
レベル2
レベル1
レベル0
0
1
2
3
4
5
6
7
8
9
終端ポイント


_stack の内容の変化
(1)
[(1, 4), V(1, 4)]
[(3, 0), V(3, 0)]
[(3, 0), V(3, 0)]
(2)
[(2, 2), V(2, 2)]
[(3, 0), V(3, 0)]
[(3, 0), V(3, 0)]
(3)
[(3, 1), V(3, 1)]
[(3, 0), V(3, 0)]
(4)
[(4, 0), V(4, 0)]

【図２５】

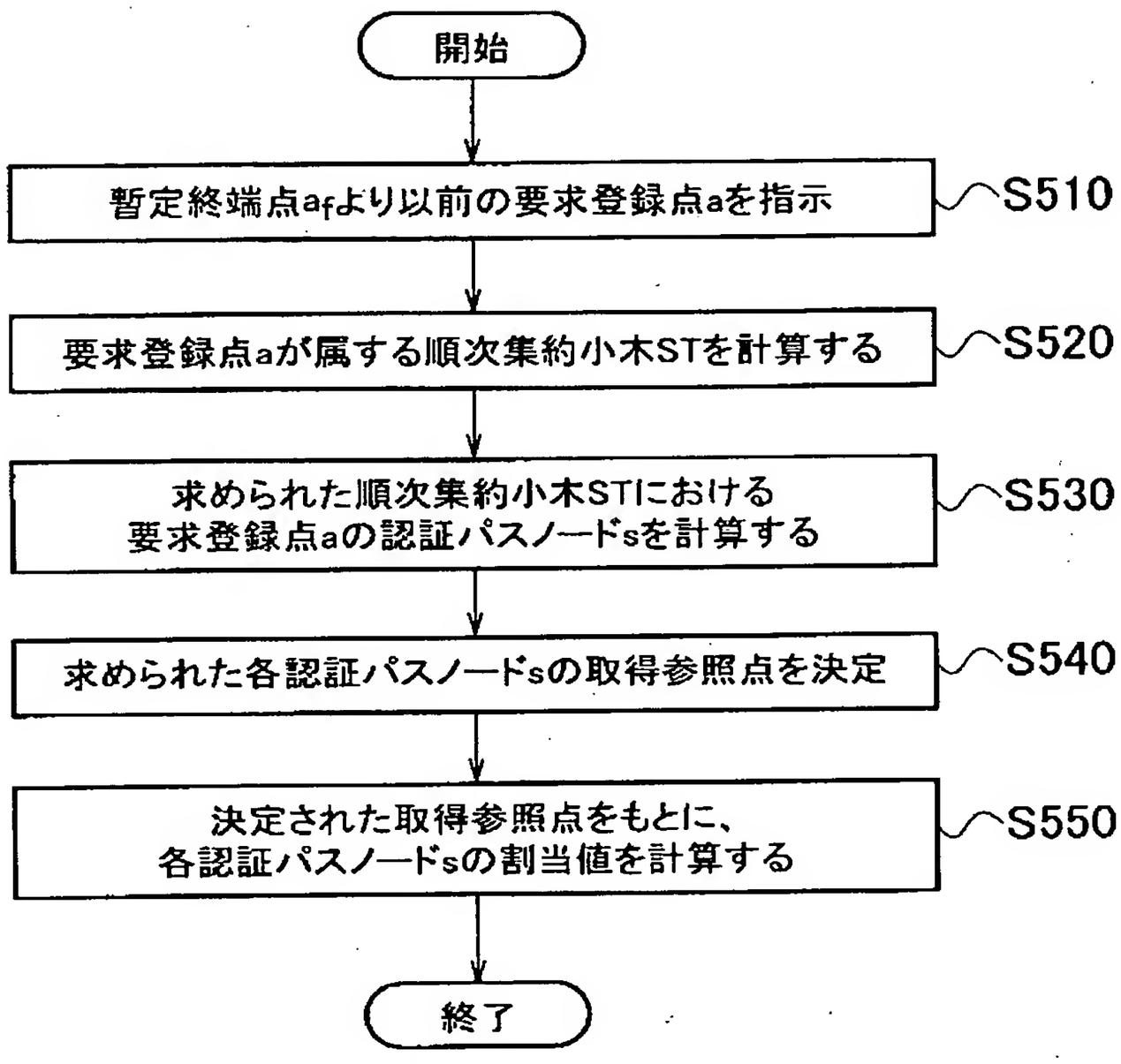


【図26】

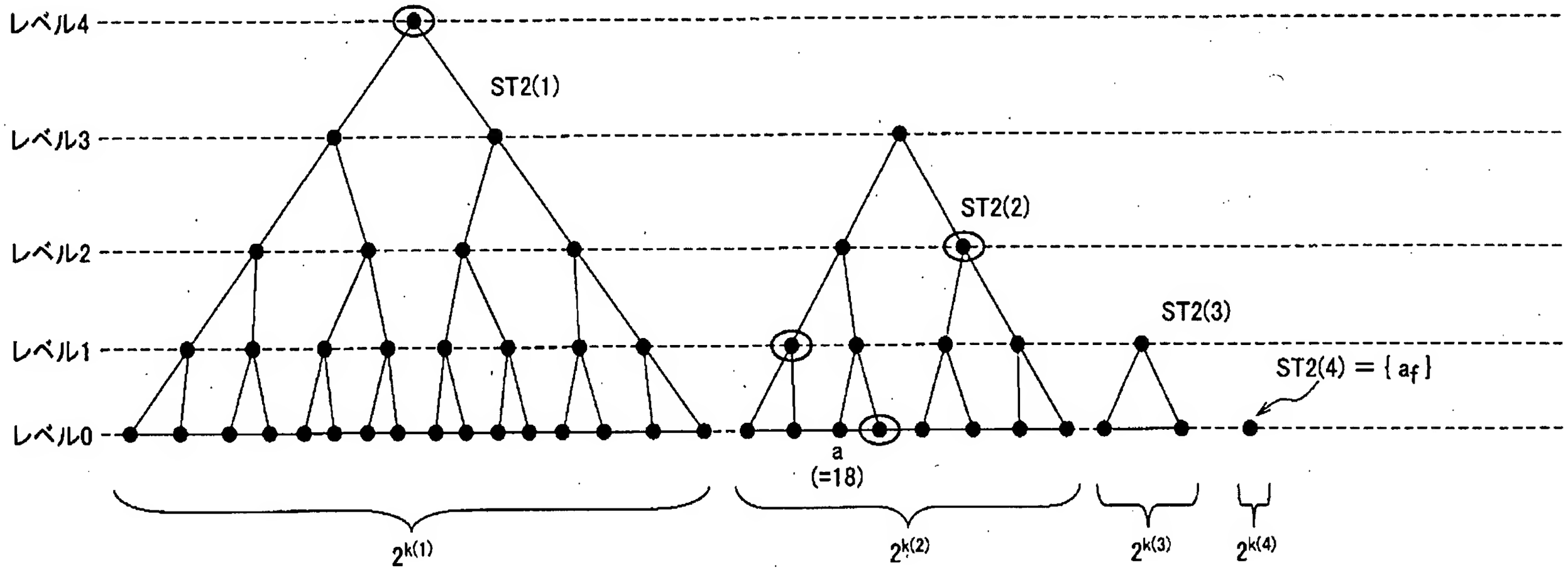


$k(1)=4 > k(2)=3 > k(3)=1 > k(4) = 0$

【図２７】

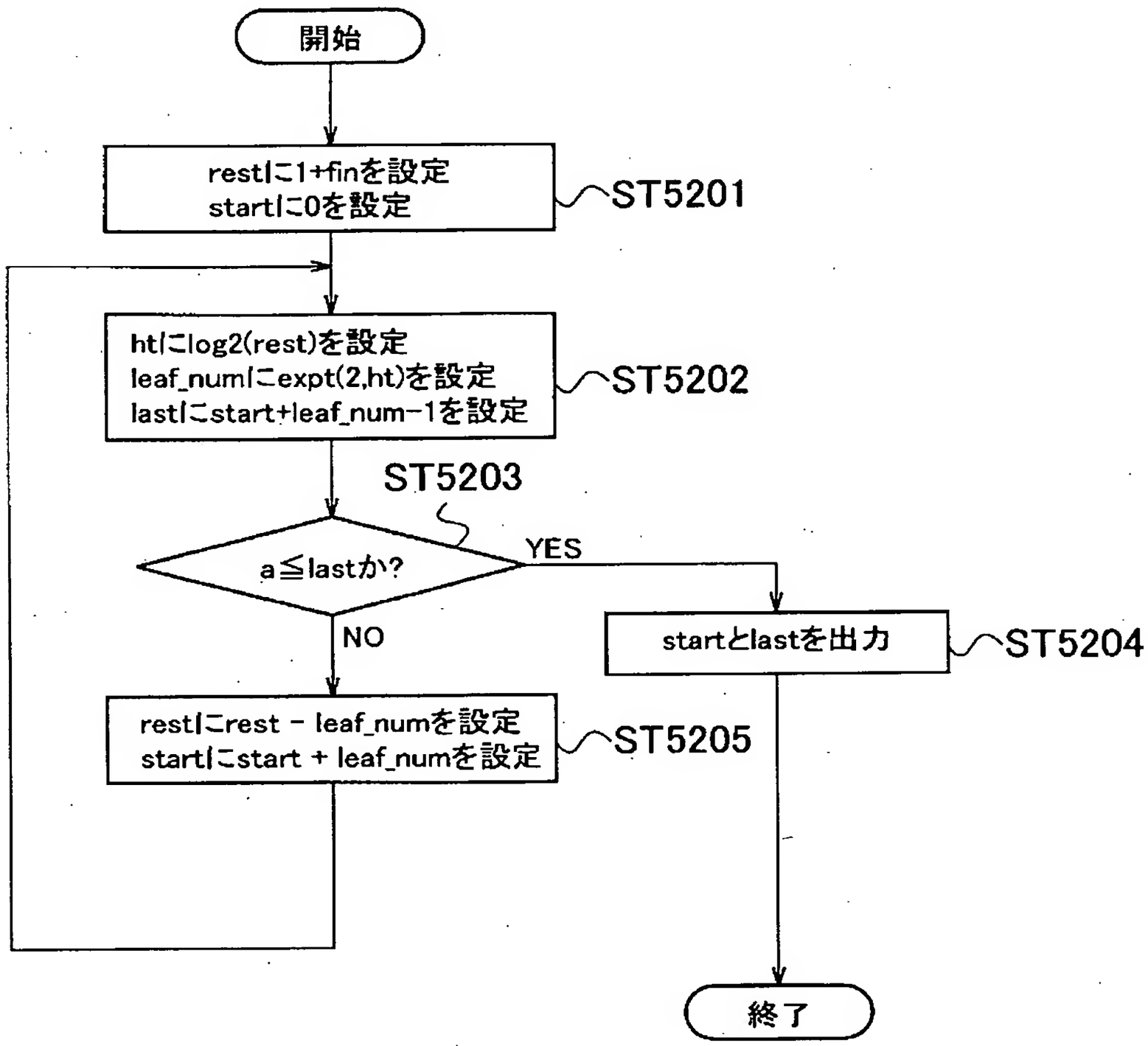

開始
暫定終端点afより以前の要求登録点aを指示
S510
要求登録点aが属する順次集約小木STを計算する
S520
求められた順次集約小木STにおける
要求登録点aの認証パスノードsを計算する
S530
求められた各認証パスノードsの取得参照点を決定
S540
決定された取得参照点をもとに、
各認証パスノードsの割当値を計算する
S550
終了

【図２８】

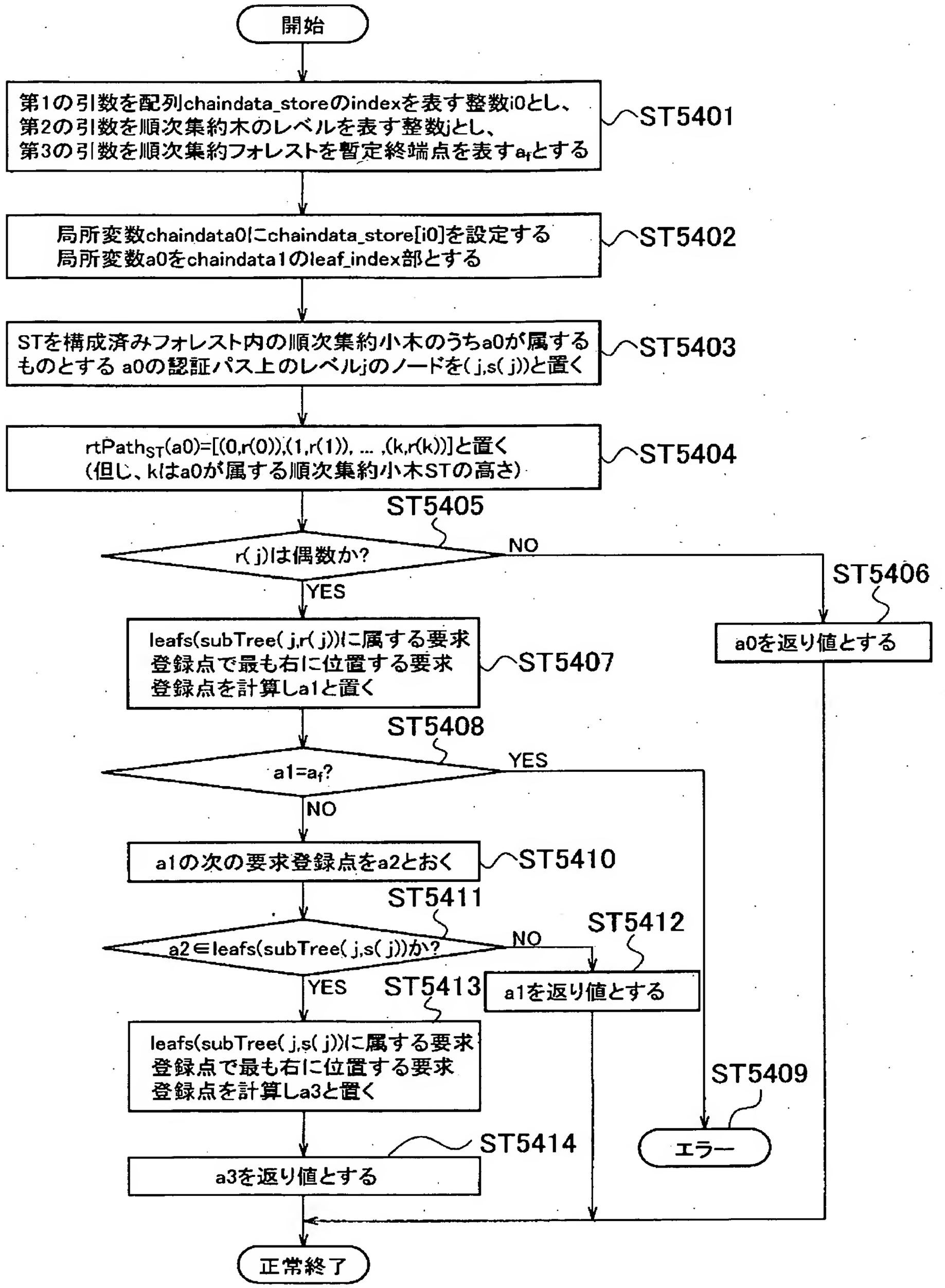


k(1)=4 >k(2)=3 >k(3)=1 >k(4)=0

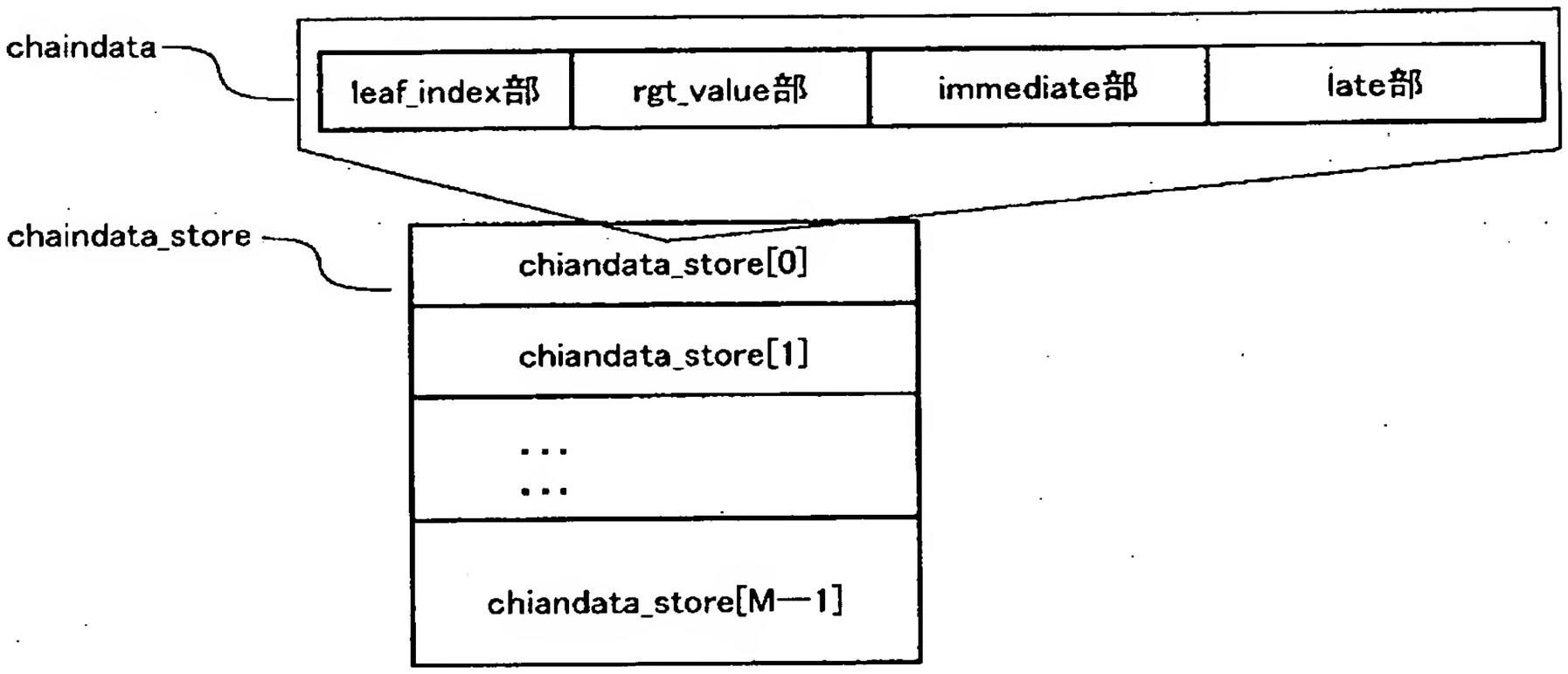
【図２９】


開始
restに1+finを設定
startに0を設定
ST5201
htにlog2(rest)を設定
leaf_numにexpt(2,ht)を設定
lastにstart+leaf_num−1を設定
ST5202
ST5203
a≦lastか?
YES
NO
startとlastを出力
ST5204
restにrest − leaf_numを設定
startにstart + leaf_numを設定
ST5205
終了

【図３０】

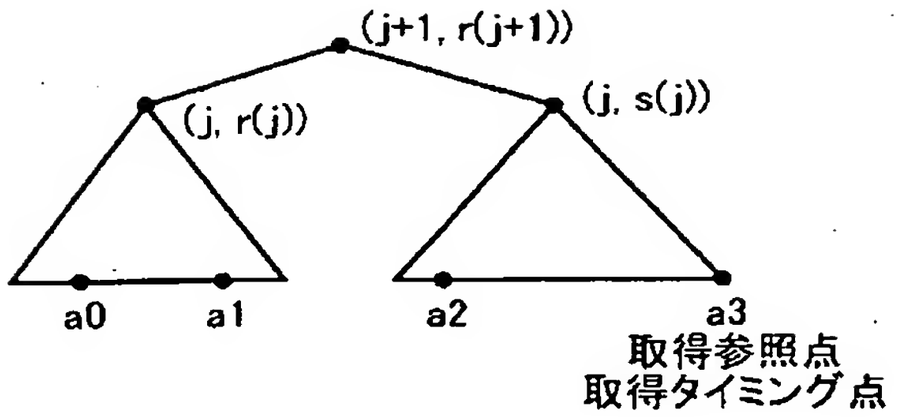

開始
第1の引数を配列chaindata_storeのindexを表す整数i0とし、
第2の引数を順次集約木のレベルを表す整数jとし、
第3の引数を順次集約フォレストを暫定終端点を表すafとする
ST5401
局所変数chaindata0にchaindata_store[i0]を設定する
局所変数a0をchaindata1のleaf_index部とする
ST5402
STを構成済みフォレスト内の順次集約小木のうちa0が属する
ものとする a0の認証パス上のレベルjのノードを(j,s(j))と置く
ST5403
rtPathST(a0)=[(0,r(0)),(1,r(1)), ... ,(k,r(k))]と置く
(但し、kはa0が属する順次集約小木STの高さ)
ST5404
ST5405
r(j)は偶数か?
NO
YES
ST5406
a0を返り値とする
leafs(subTree(j,r(j))に属する要求
登録点で最も右に位置する要求
登録点を計算しa1と置く
ST5407
ST5408
a1=af?
YES
NO
a1の次の要求登録点をa2とおく
ST5410
ST5411
a2∈leafs(subTree(j,s(j))か?
NO
ST5412
YES
ST5413
a1を返り値とする
leafs(subTree(j,s(j))に属する要求
登録点で最も右に位置する要求
登録点を計算しa3と置く
ST5414
a3を返り値とする
ST5409
エラー
正常終了

【図３１】

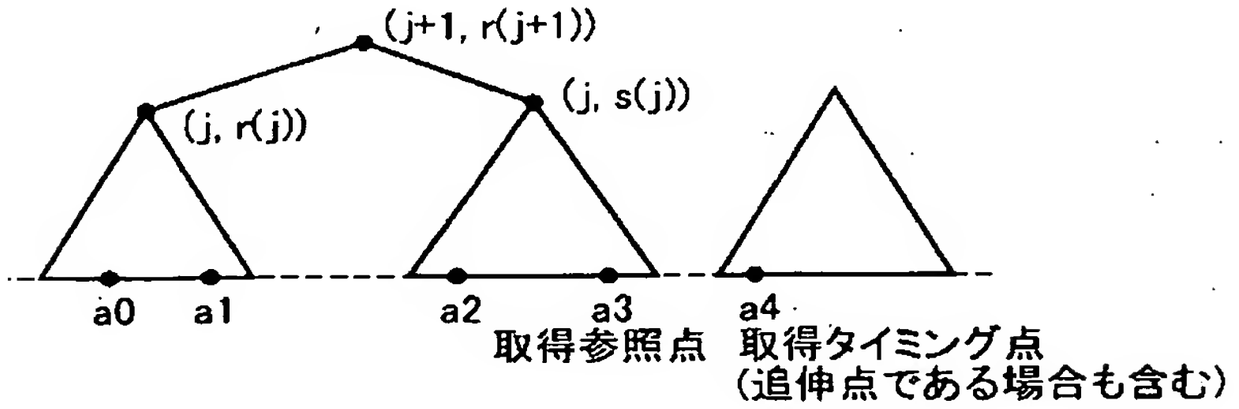

chaindata
leaf_index部
rgt_value部
immediate部
late部
chaindata_store
chiandata_store[0]
chiandata_store[1]
・・・
・・・
chiandata_store[M−1]

【図３２】

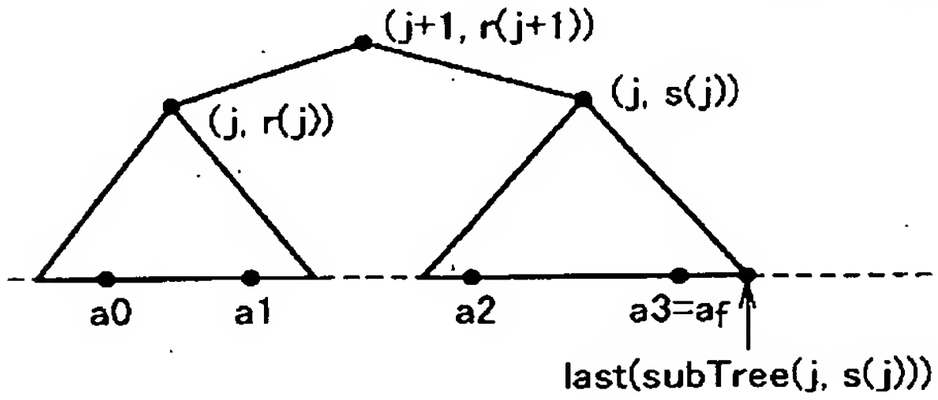
(a)


(j+1, r(j+1))
(j, r(j))
(j, s(j))
a0
a1
a2
a3
取得参照点
取得タイミング点

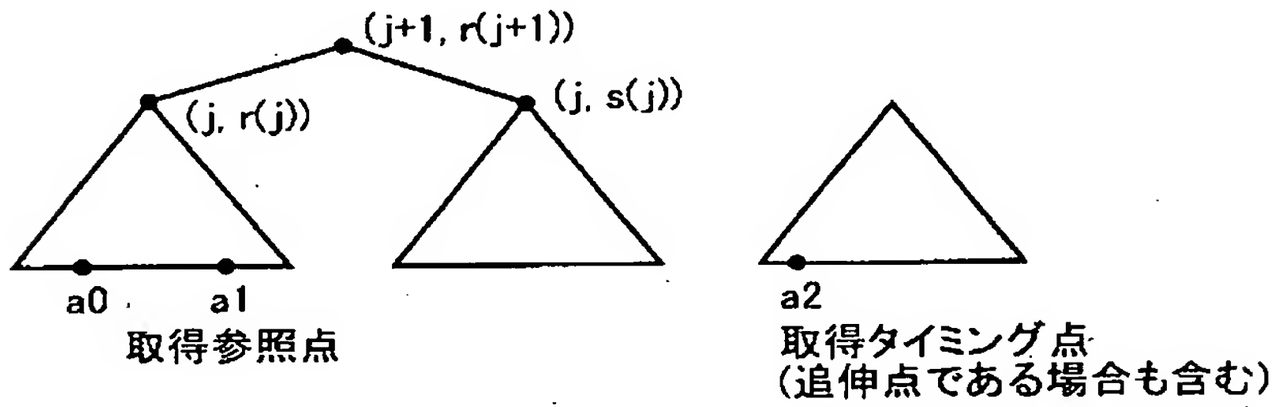
(b)


(j+1, r(j+1))
(j, r(j))
(j, s(j))
a0
a1
a2
a3
a4
取得参照点
取得タイミング点
(追伸点である場合も含む)

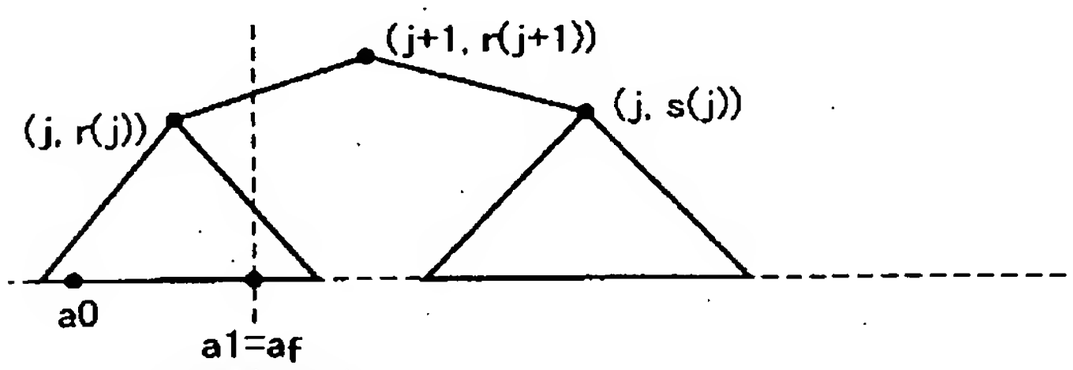
(c)


(j+1, r(j+1))
(j, r(j))
(j, s(j))
a0
a1
a2
a3=af
last(subTree(j, s(j)))

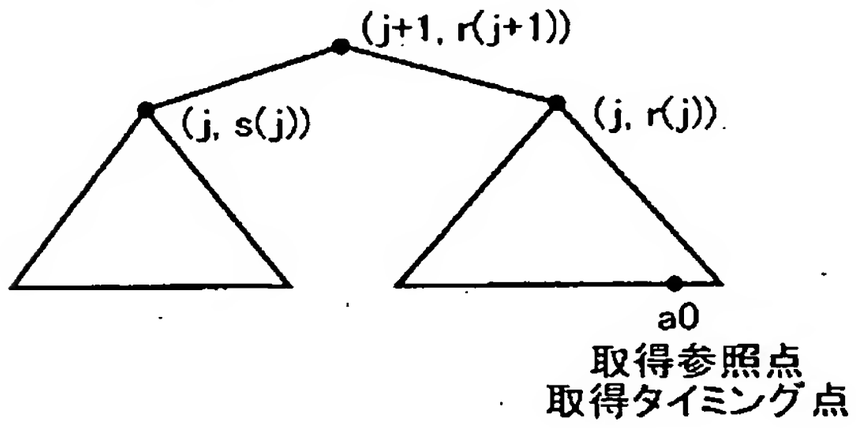
(d)


(j+1, r(j+1))
(j, r(j))
(j, s(j))
a0
a1
取得参照点
a2
取得タイミング点
(追伸点である場合も含む)

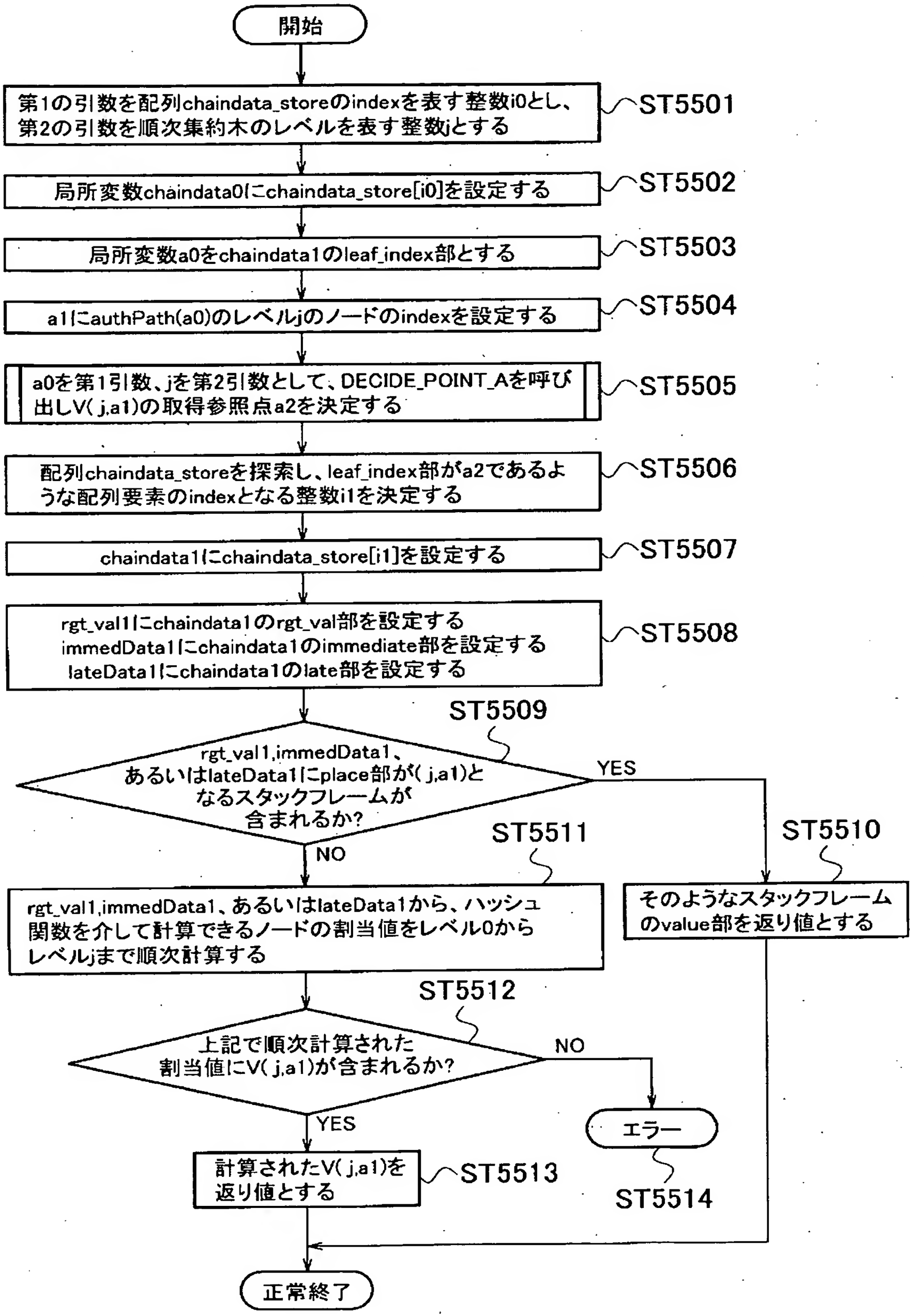
(e)


(j+1, r(j+1))
(j, r(j))
(j, s(j))
a0
a1=af

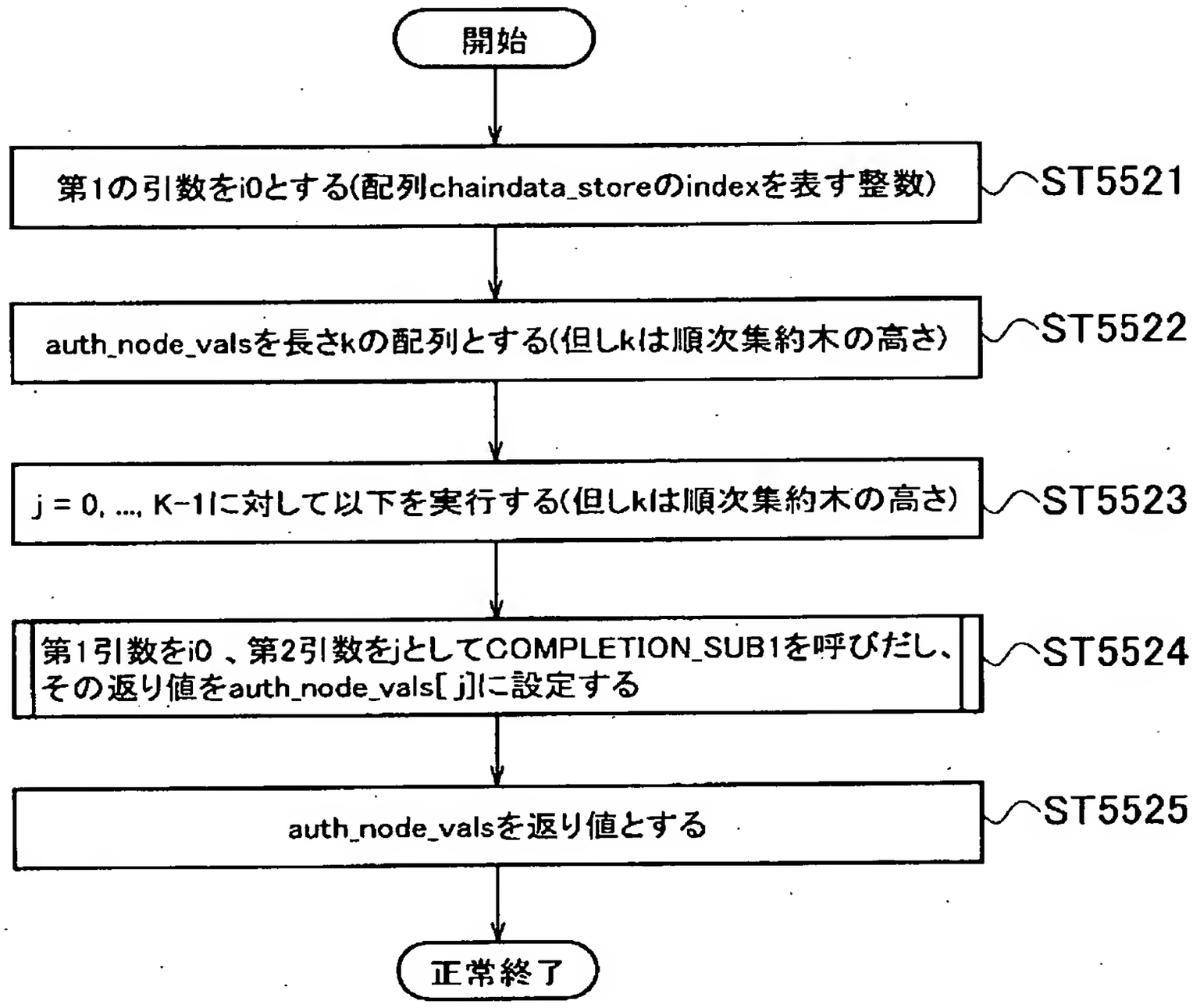
(f)


取得参照点
(j+1, r(j+1))
(j, s(j))
(j, r(j))
a0
取得参照点
取得タイミング点

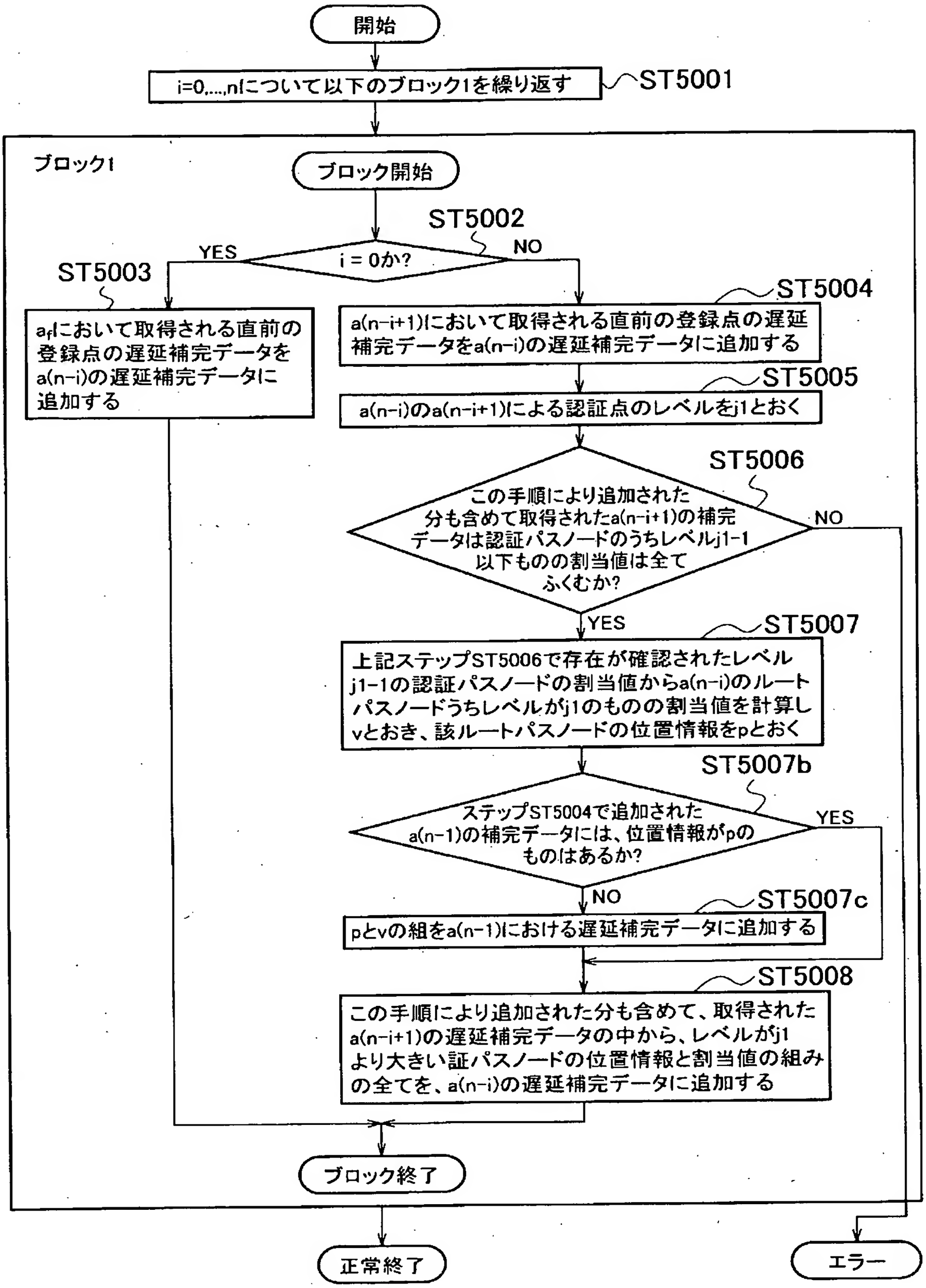
【図３３】


開始
第1の引数を配列chaindata_storeのindexを表す整数i0とし、第2の引数を順次集約木のレベルを表す整数jとする
ST5501
局所変数chaindata0にchaindata_store[i0]を設定する
ST5502
局所変数a0をchaindata1のleaf_index部とする
ST5503
a1にauthPath(a0)のレベルjのノードのindexを設定する
ST5504
a0を第1引数、jを第2引数として、DECIDE_POINT_Aを呼び出しV(j,a1)の取得参照点a2を決定する
ST5505
配列chaindata_storeを探索し、leaf_index部がa2であるような配列要素のindexとなる整数i1を決定する
ST5506
chaindata1にchaindata_store[i1]を設定する
ST5507
rgt_val1にchaindata1のrgt_val部を設定する
immedData1にchaindata1のimmediate部を設定する
lateData1にchaindata1のlate部を設定する
ST5508
ST5509
rgt_val1,immedData1、あるいはlateData1にplace部が(j,a1)となるスタックフレームが含まれるか?
YES
NO
ST5510
そのようなスタックフレームのvalue部を返り値とする
ST5511
rgt_val1,immedData1、あるいはlateData1から、ハッシュ関数を介して計算できるノードの割当値をレベル0からレベルjまで順次計算する
ST5512
上記で順次計算された割当値にV(j,a1)が含まれるか?
NO
YES
エラー
ST5514
計算されたV(j,a1)を返り値とする
ST5513
正常終了

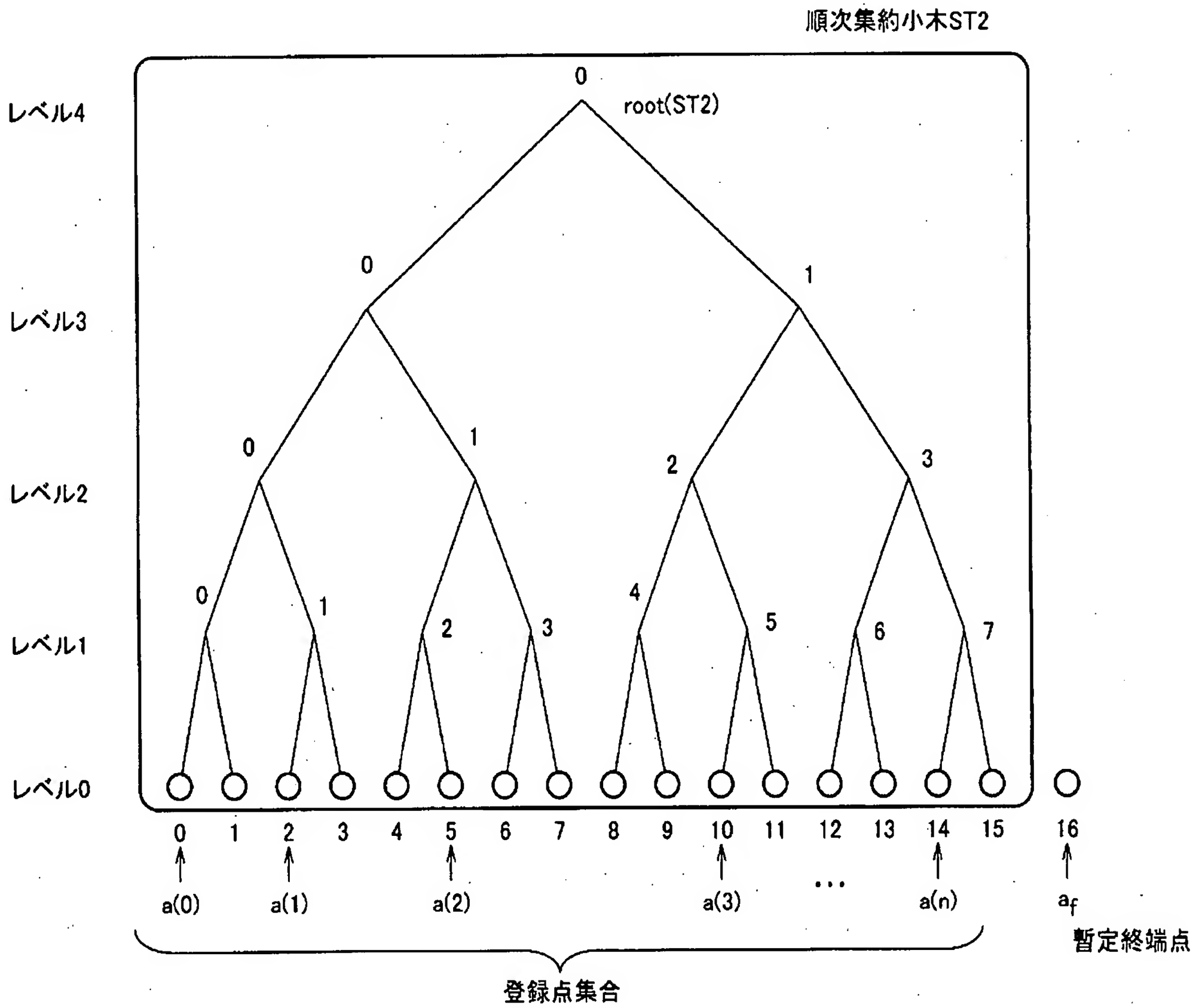
【図３４】


開始
第1の引数をi0とする(配列chaindata_storeのindexを表す整数)
ST5521
auth_node_valsを長さkの配列とする(但しkは順次集約木の高さ)
ST5522
j = 0, ..., K-1に対して以下を実行する(但しkは順次集約木の高さ)
ST5523
第1引数をi0 、第2引数をjとしてCOMPLETION_SUB1を呼びだし、
その返り値をauth_node_vals[j]に設定する
ST5524
auth_node_valsを返り値とする
ST5525
正常終了

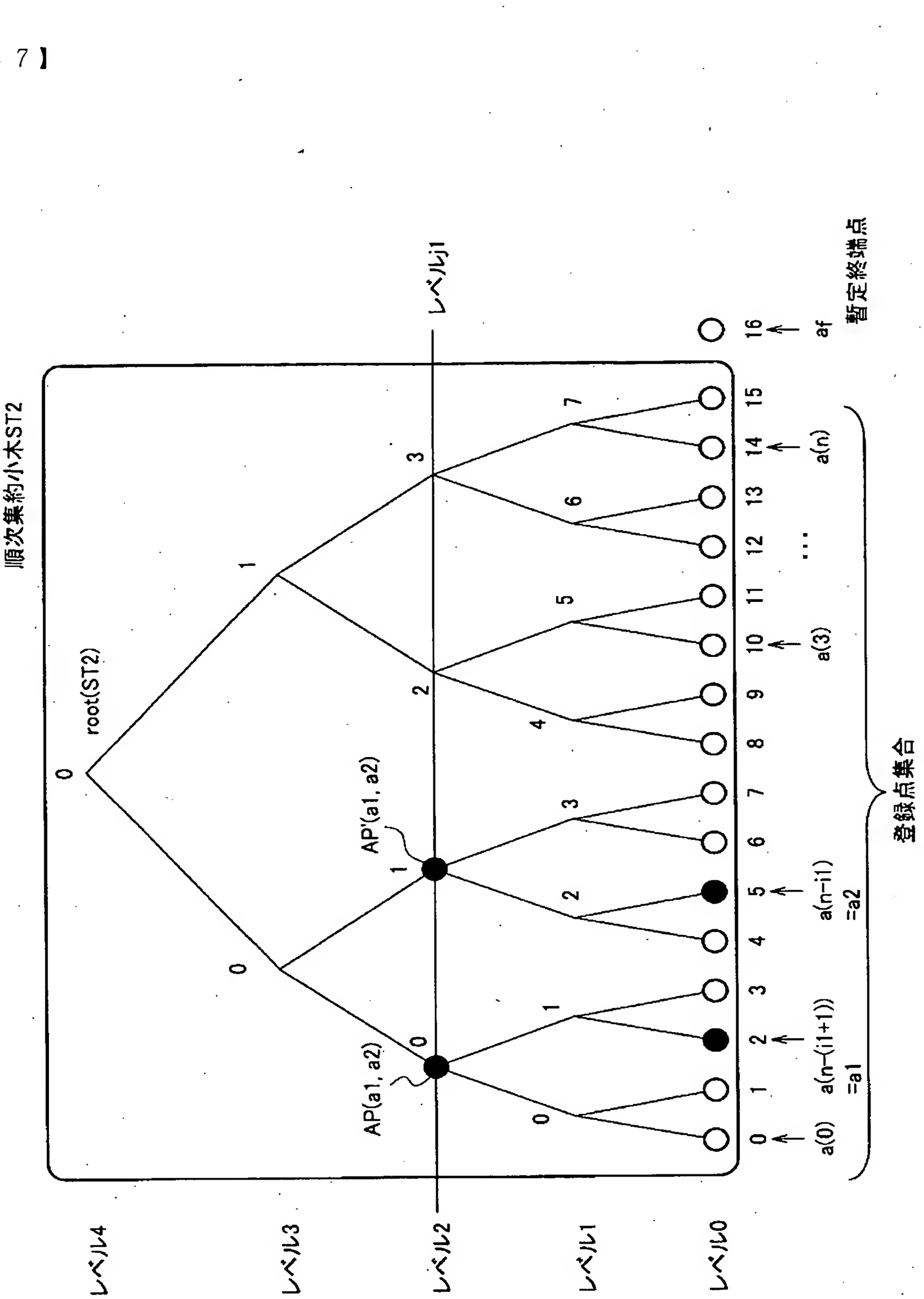
【図３５】


開始
i=0,...,nについて以下のブロック1を繰り返す
ST5001
ブロック1
ブロック開始
ST5002
YES
i = 0か?
NO
ST5003
afiにおいて取得される直前の登録点の遅延補完データをa(n-i)の遅延補完データに追加する
ST5004
a(n-i+1)において取得される直前の登録点の遅延補完データをa(n-i)の遅延補完データに追加する
ST5005
a(n-i)のa(n-i+1)による認証点のレベルをj1とおく
ST5006
この手順により追加された分も含めて取得されたa(n-i+1)の補完データは認証パスノードのうちレベルj1-1以下ものの割当値は全てふくむか?
NO
YES
ST5007
上記ステップST5006で存在が確認されたレベルj1-1の認証パスノードの割当値からa(n-i)のルートパスノードうちレベルがj1のものの割当値を計算しvとおき、該ルートパスノードの位置情報をpとおく
ST5007b
ステップST5004で追加されたa(n-1)の補完データには、位置情報がpのものはあるか?
YES
NO
ST5007c
pとvの組をa(n-1)における遅延補完データに追加する
ST5008
この手順により追加された分も含めて、取得されたa(n-i+1)の遅延補完データの中から、レベルがj1より大きい証パスノードの位置情報と割当値の組みの全てを、a(n-i)の遅延補完データに追加する
ブロック終了
正常終了
エラー

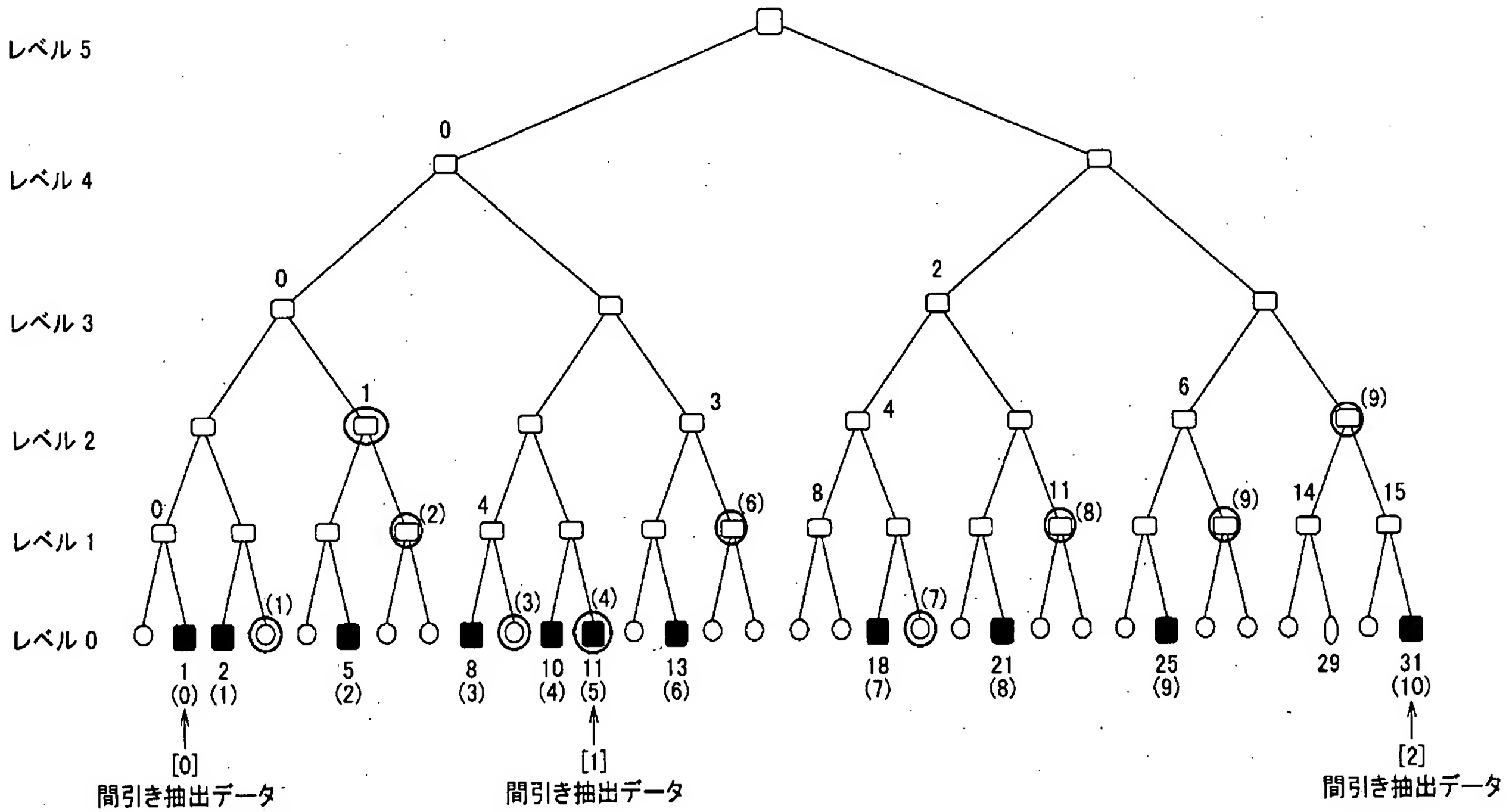
【図３６】


順次集約小木ST2
レベル4
レベル3
レベル2
レベル1
レベル0
root(ST2)
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
a(0) a(1) a(2) a(3) ... a(n) af
暫定終端点
登録点集合

【図３７】

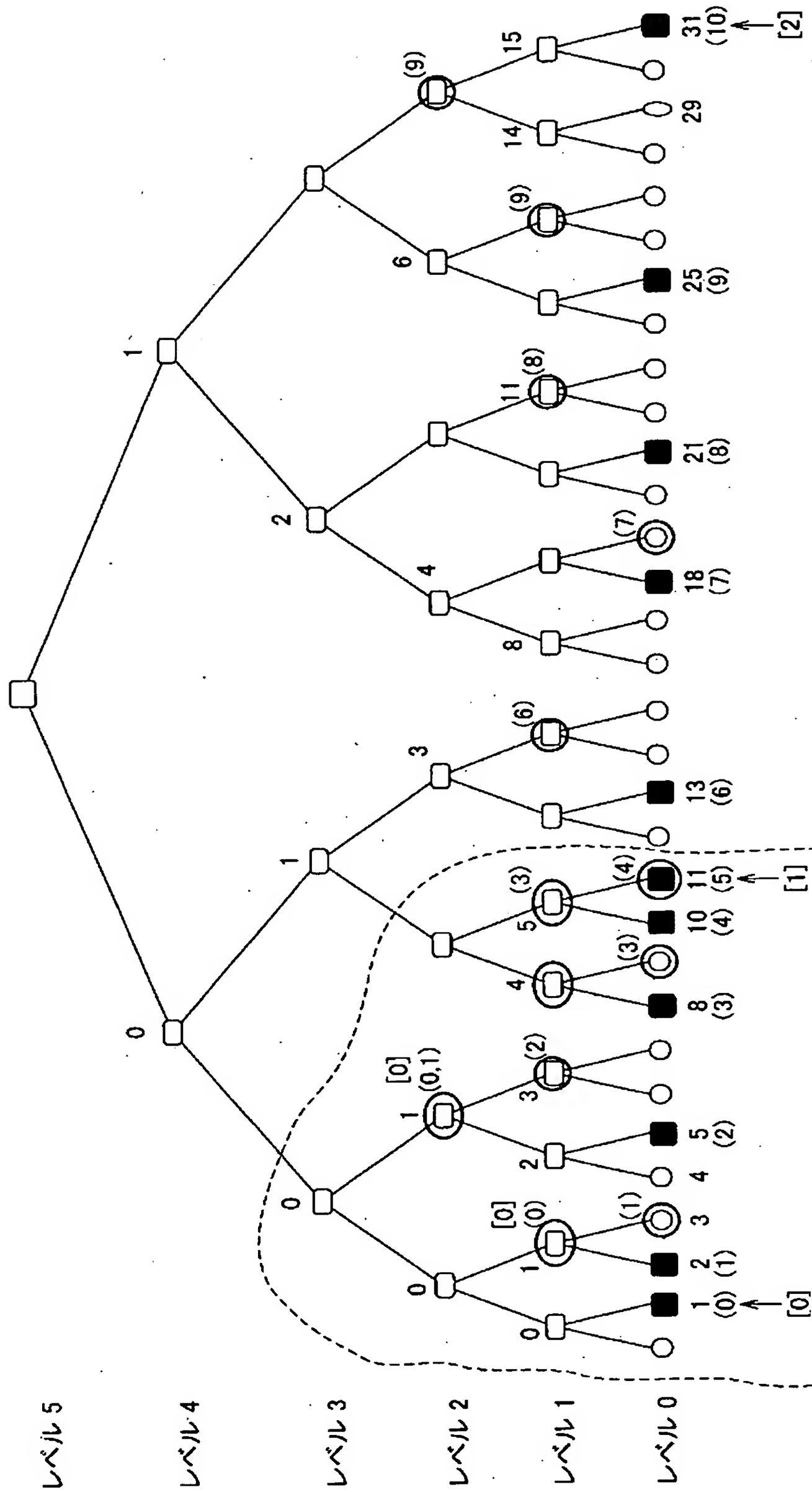

順次集約小木ST2
レベルj1
root(ST2)
AP(a1, a2)
AP'(a1, a2)
a(0)
a(n−(i1+1))
=a1
a(n−i1)
=a2
a(3)
af
暫定終端点
登録点集合
レベル4
レベル3
レベル2
レベル1
レベル0

【図３８】

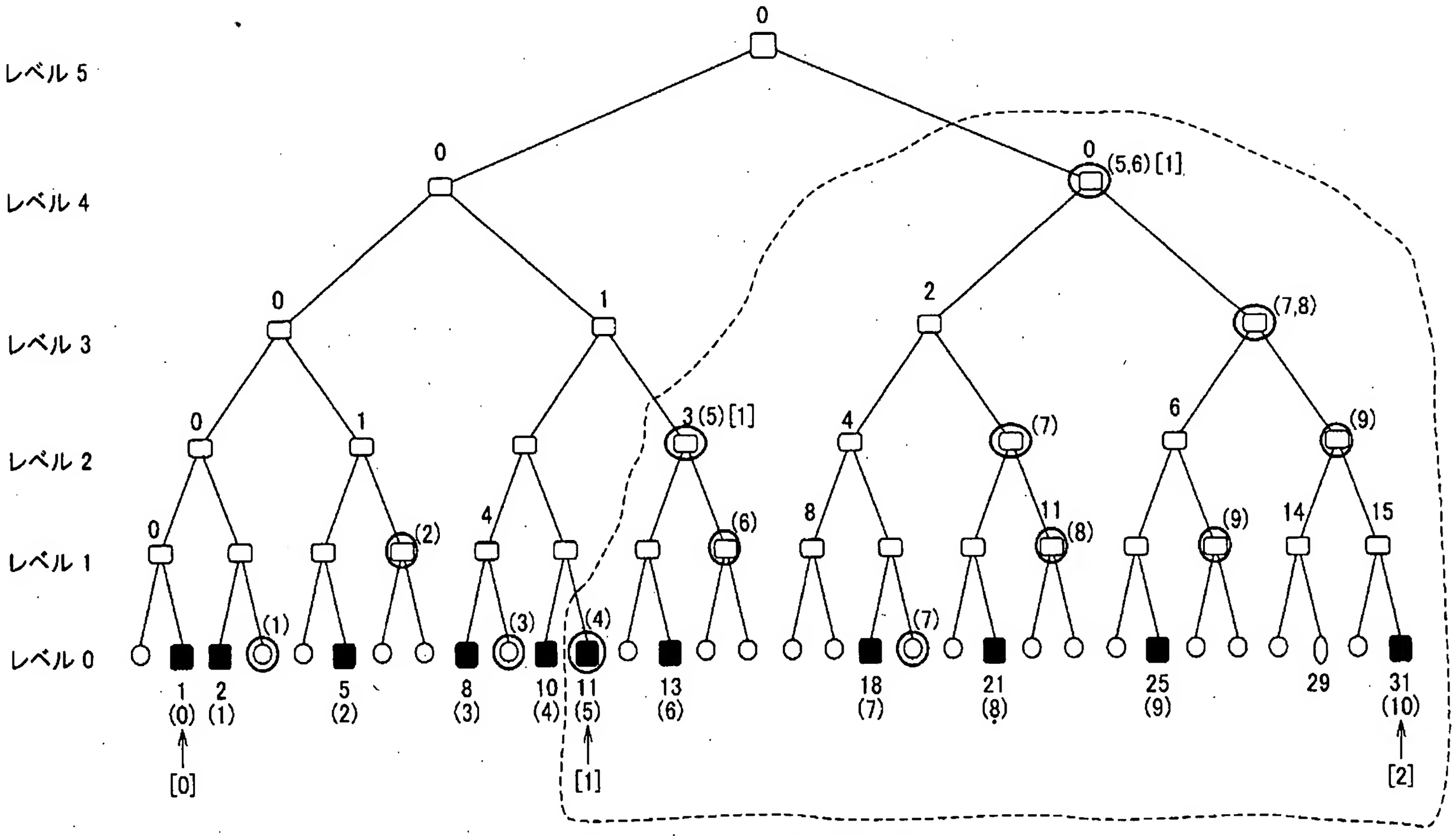


間引き抽出データインデックス[0..2]の設定

【図３９】

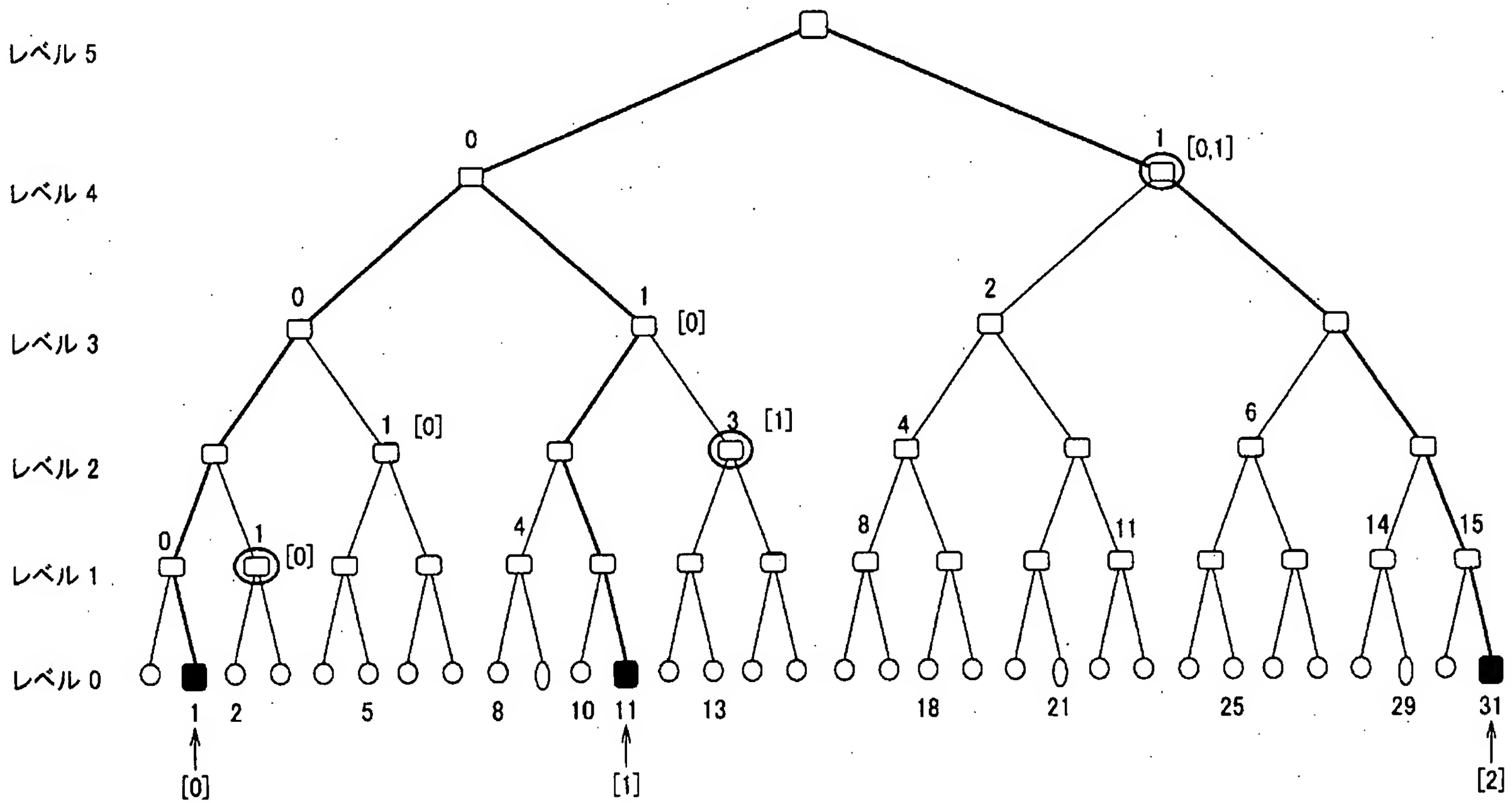

レベル５
レベル４
レベル３
レベル２
レベル１
レベル０
第1の局所データの局所完全化の結果
局所完全化の元のインデックスの範囲[0..5]
間引き抽出データインデックスの範囲[0..1]

【図４０】

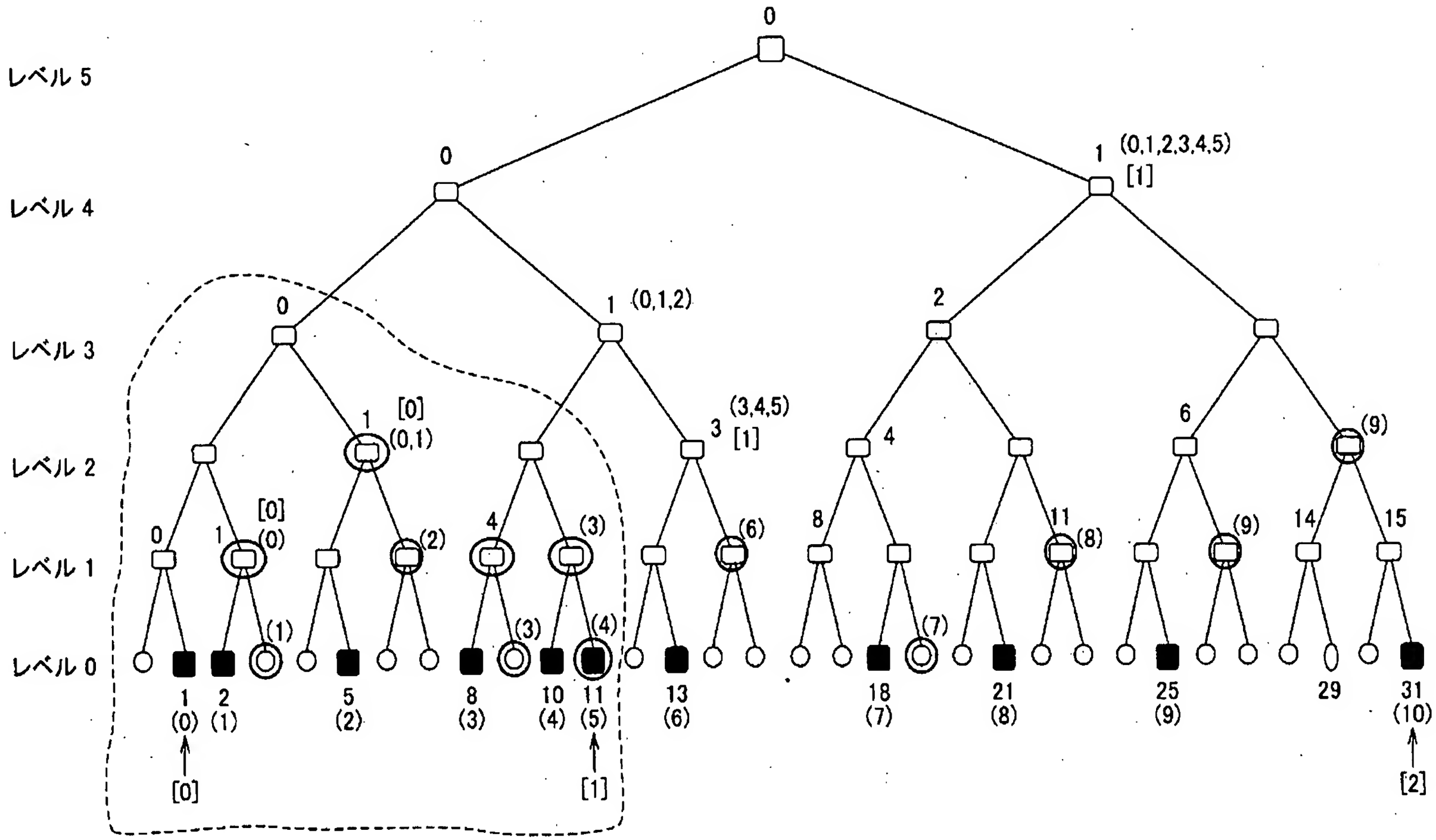


第2の局所データの局所完全化の結果
局所完全化のインデックスの範囲[5..10]
間引き抽出データインデックスの範囲[1..2]

【図４１】

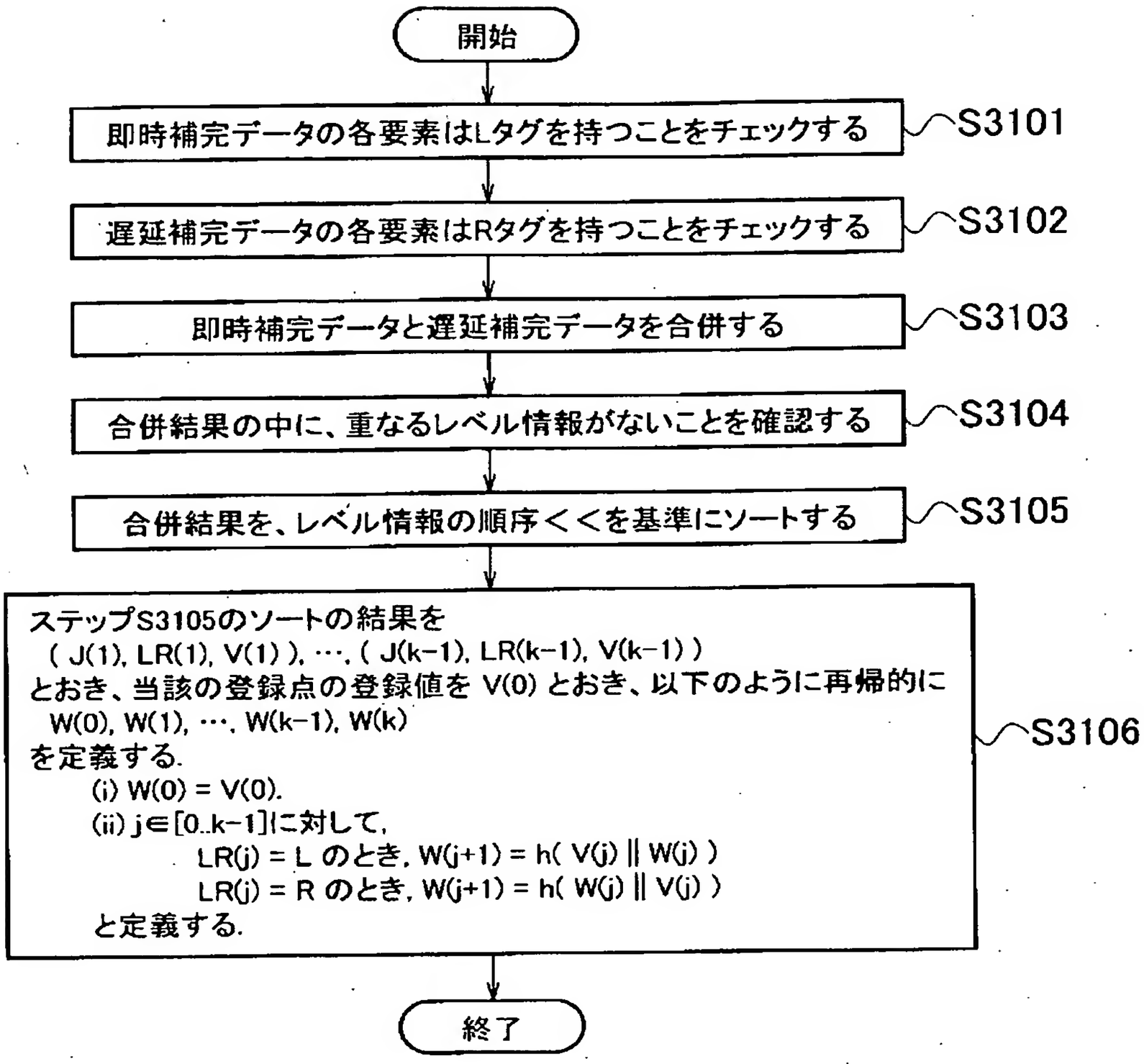

レベル 5
レベル 4
レベル 3
レベル 2
レベル 1
レベル 0
0
1 [0,1]
0
1 [0]
2
0
1 [0]
3 [1]
4
6
0
1 [0]
4
8
11
14
15
1
2
5
8
10
11
13
18
21
25
29
31
[0]
[1]
[2]

【図４２】

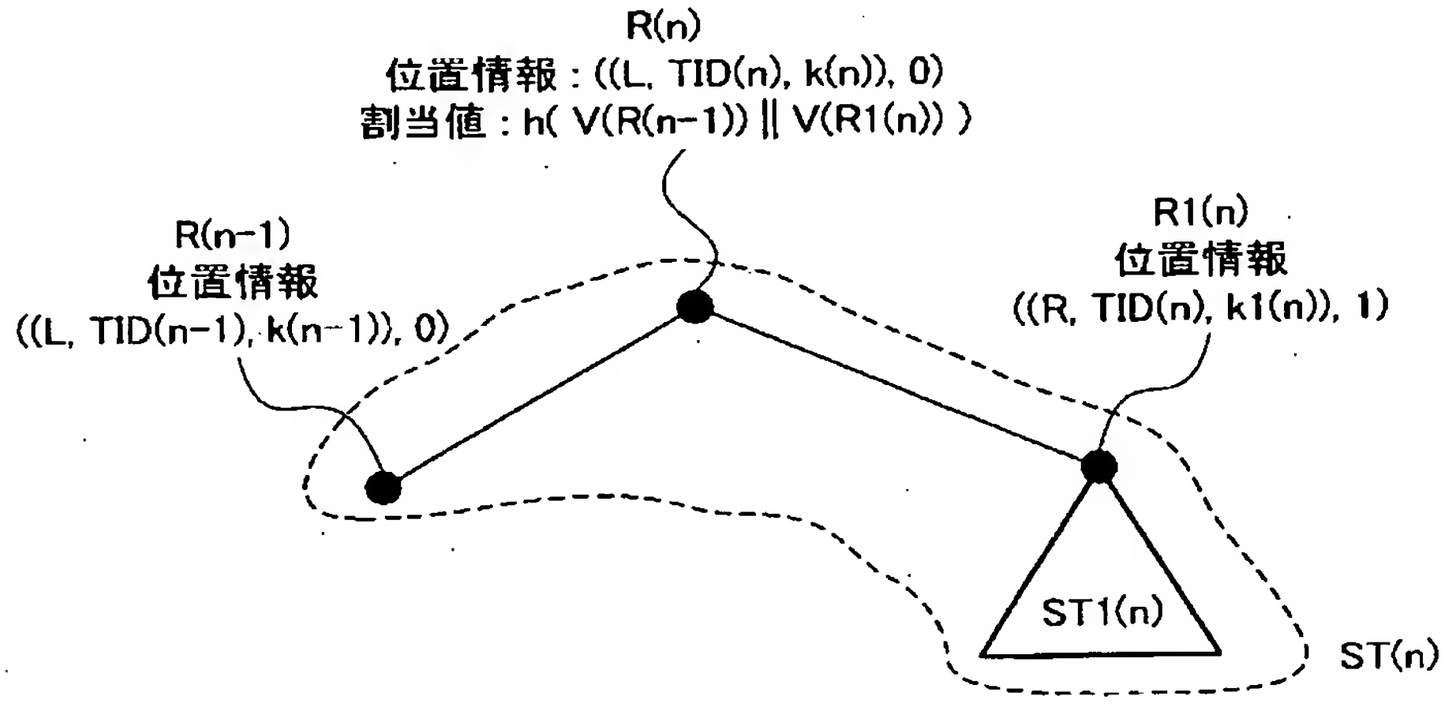


第1の局所データの大域完全化の結果
局所完全化のインデックスの範囲[0..5]

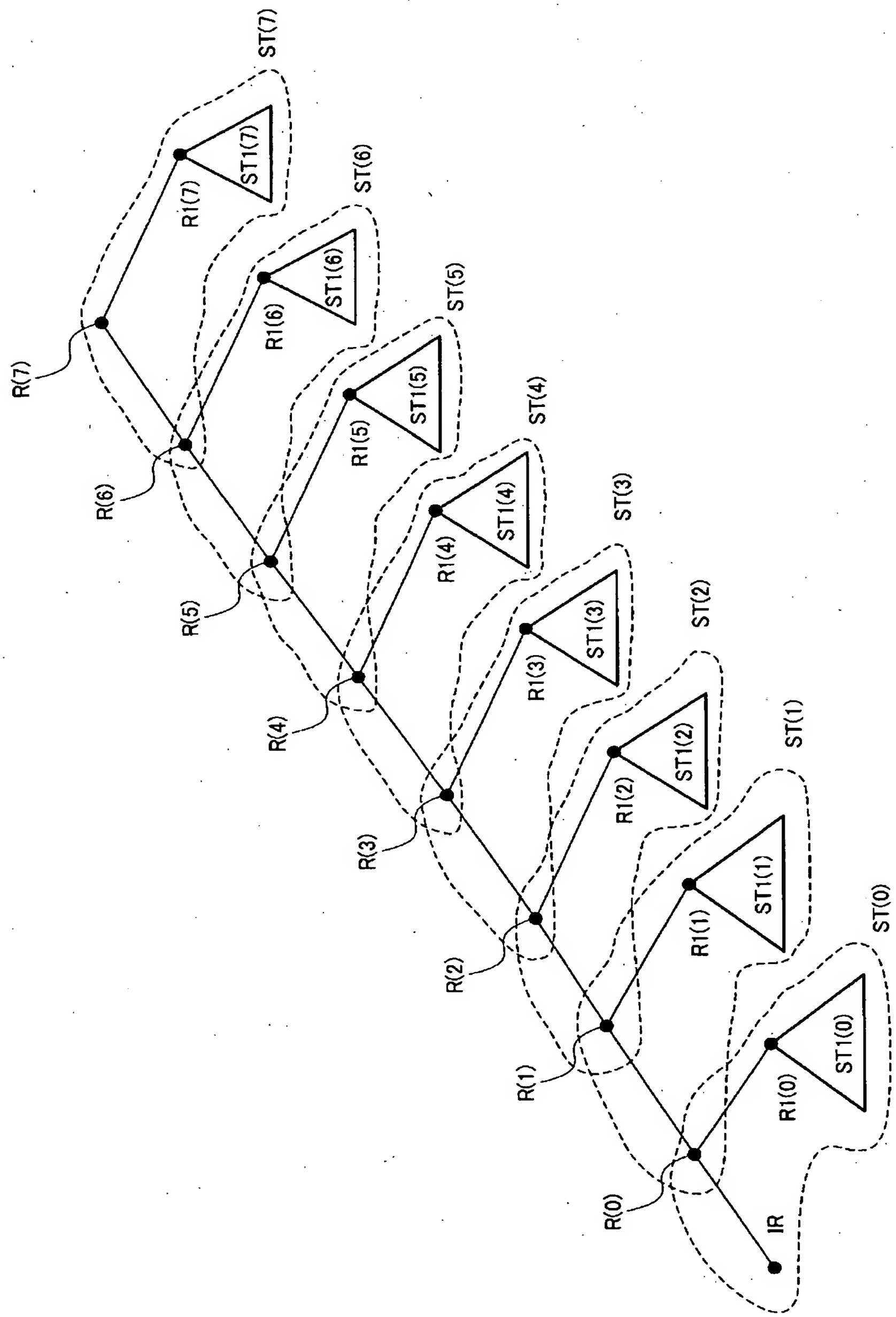
【図４３】


開始
即時補完データの各要素はLタグを持つことをチェックする
S3101
遅延補完データの各要素はRタグを持つことをチェックする
S3102
即時補完データと遅延補完データを合併する
S3103
合併結果の中に、重なるレベル情報がないことを確認する
S3104
合併結果を、レベル情報の順序＜＜を基準にソートする
S3105
ステップS3105のソートの結果を
(J(1), LR(1), V(1)), …, (J(k−1), LR(k−1), V(k−1))
とおき、当該の登録点の登録値を V(0) とおき、以下のように再帰的に
W(0), W(1), …, W(k−1), W(k)
を定義する.
(i) W(0) = V(0).
(ii) j∈[0..k−1]に対して,
LR(j) = L のとき, W(j+1) = h(V(j) || W(j))
LR(j) = R のとき, W(j+1) = h(W(j) || V(j))
と定義する.
S3106
終了

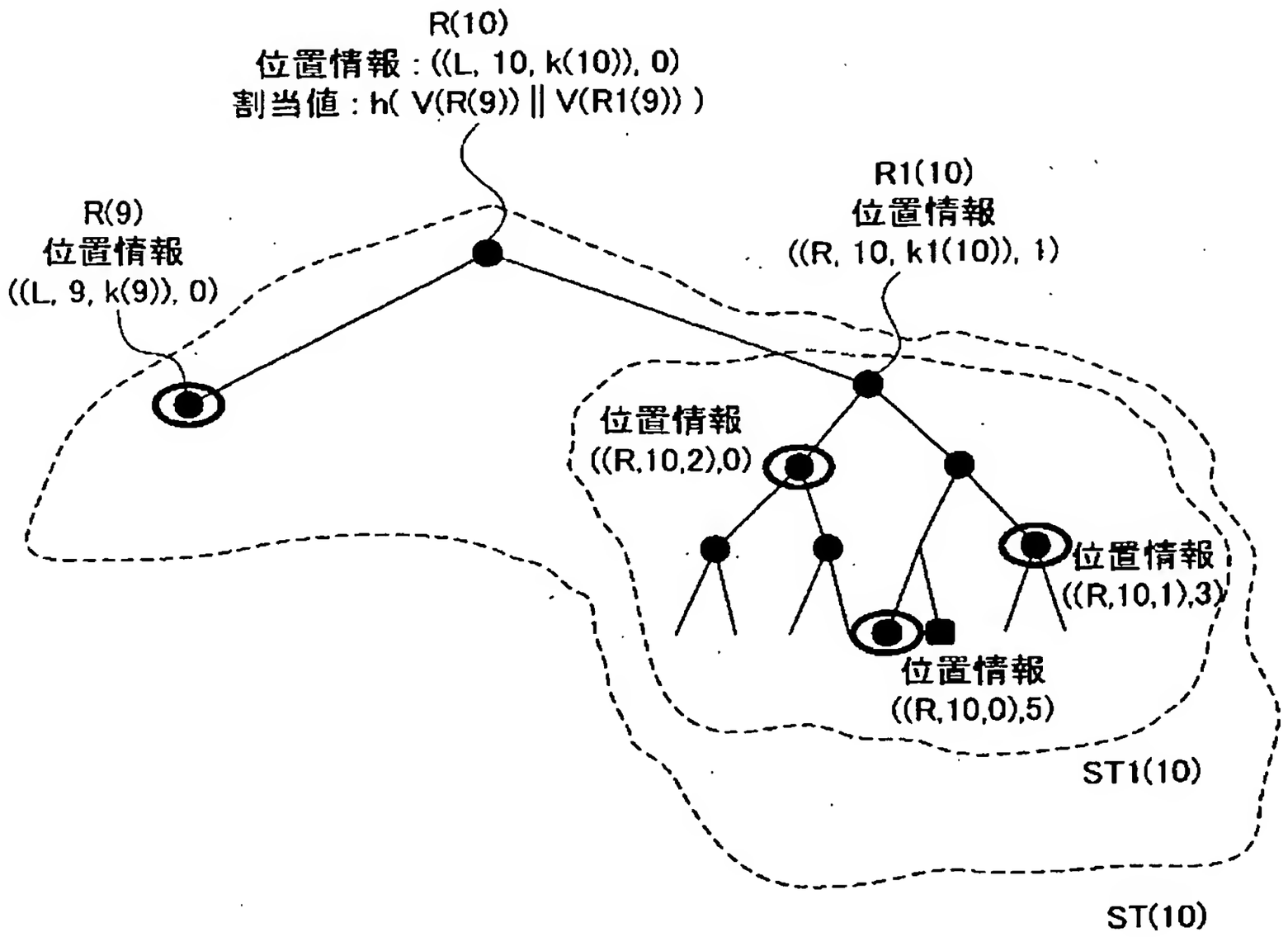
【図４４】


R(n)
位置情報：((L, TID(n), k(n)), 0)
割当値：h(V(R(n−1)) || V(R1(n)))
R(n−1)
位置情報
((L, TID(n−1), k(n−1)), 0)
R1(n)
位置情報
((R, TID(n), k1(n)), 1)
ST1(n)
ST(n)

【図４５】

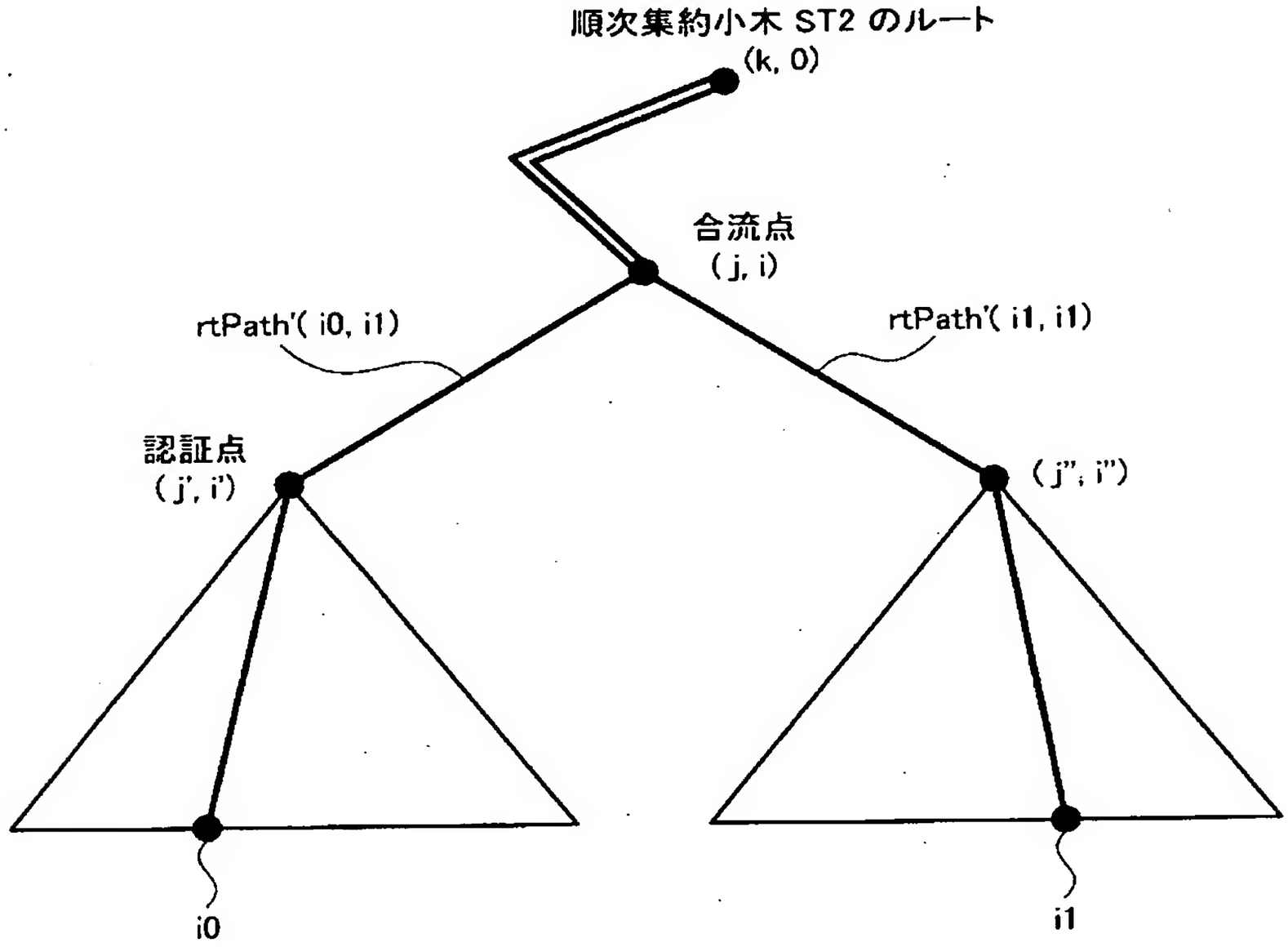

R(7)
R1(7)
ST1(7)
ST(7)
R(6)
R1(6)
ST1(6)
ST(6)
R(5)
R1(5)
ST1(5)
ST(5)
R(4)
R1(4)
ST1(4)
ST(4)
R(3)
R1(3)
ST1(3)
ST(3)
R(2)
R1(2)
ST1(2)
ST(2)
R(1)
R1(1)
ST1(1)
ST(1)
R(0)
R1(0)
ST1(0)
ST(0)
IR

【図４６】


R(10)
位置情報：((L, 10, k(10)), 0)
割当値：h(V(R(9)) || V(R1(9)))
R(9)
位置情報
((L, 9, k(9)), 0)
R1(10)
位置情報
((R, 10, k1(10)), 1)
位置情報
((R,10,2),0)
位置情報
((R,10,1),3)
位置情報
((R,10,0),5)
ST1(10)
ST(10)

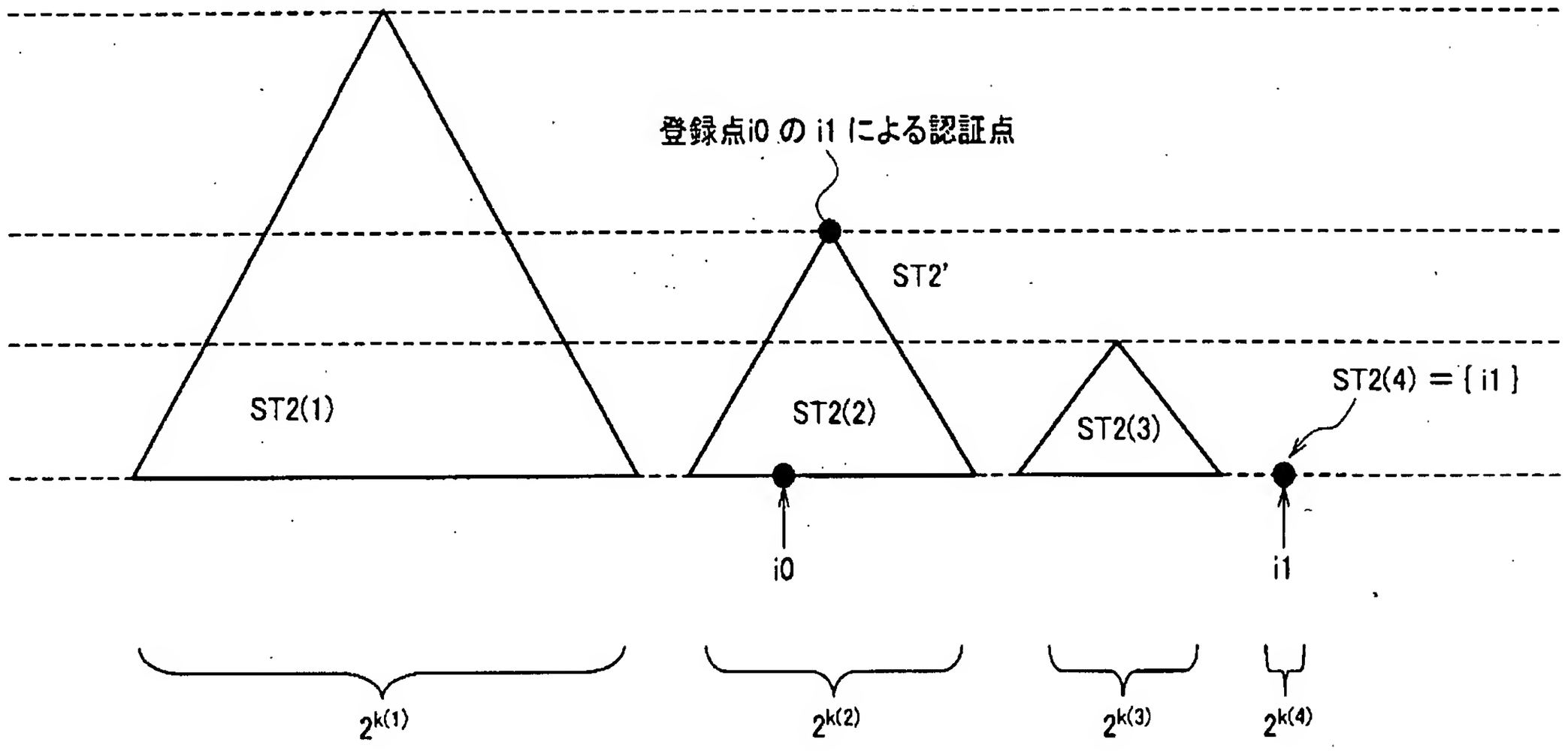
【図４７】

i0 と i1 がi1時点における1つの順次集約小木に属するとき



【図４８】

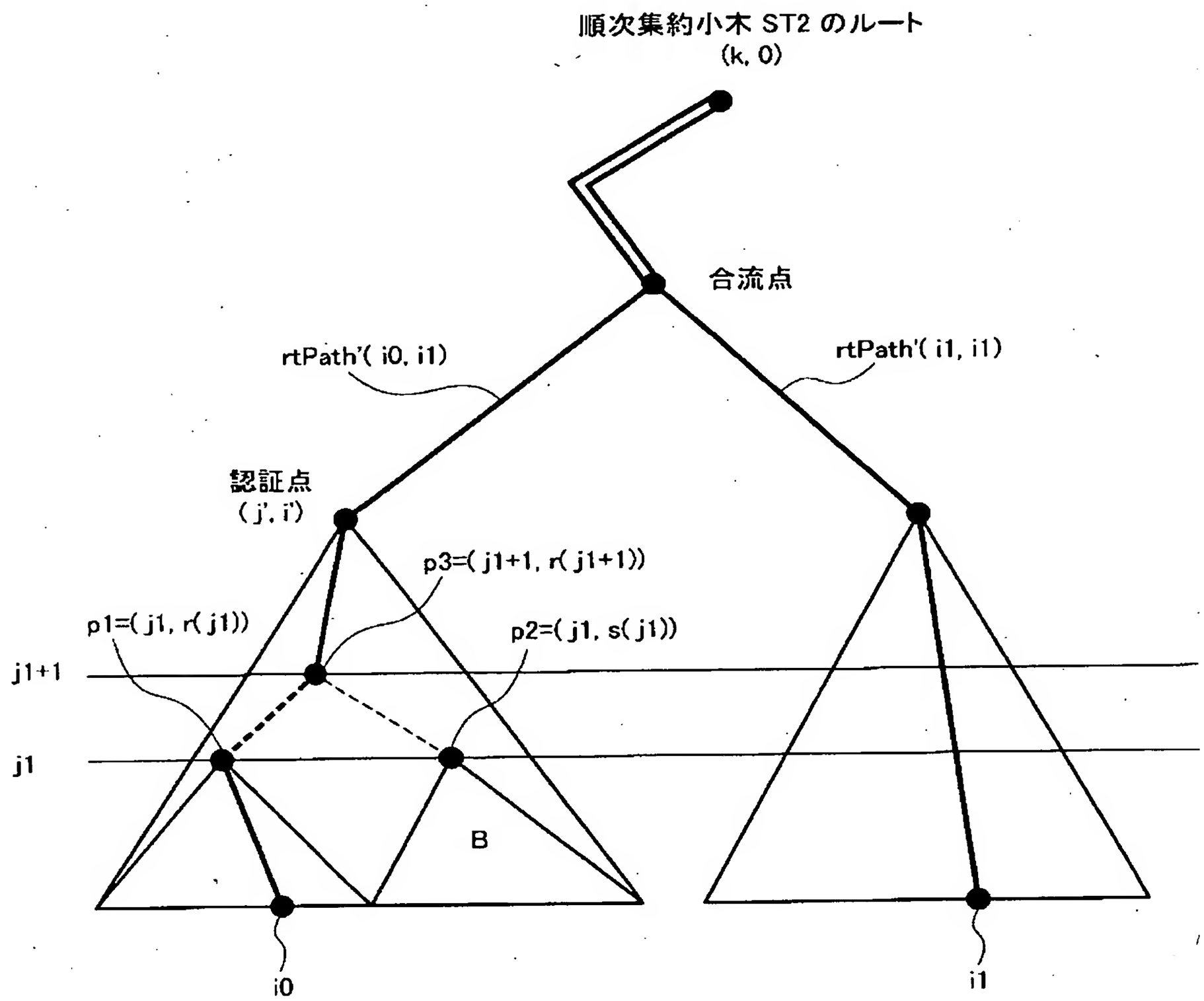
i0 と i1 がi1時点における1つの順次集約小木に属さないとき



$k(1) > k(2) > k(3) > k(4) = 0$

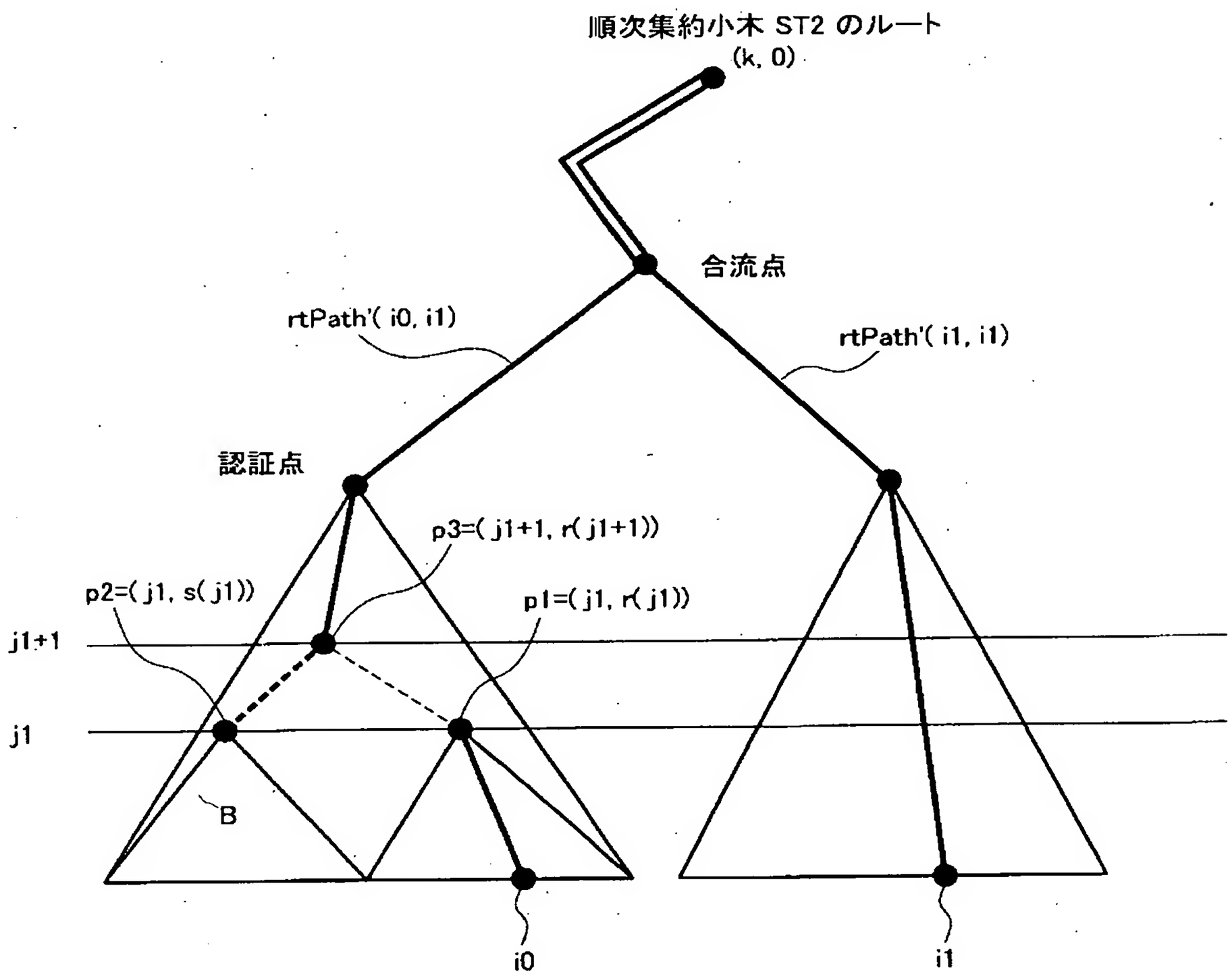
【図４９】

i0 と i1 がi1時点における1つの順次集約小木に属するとき



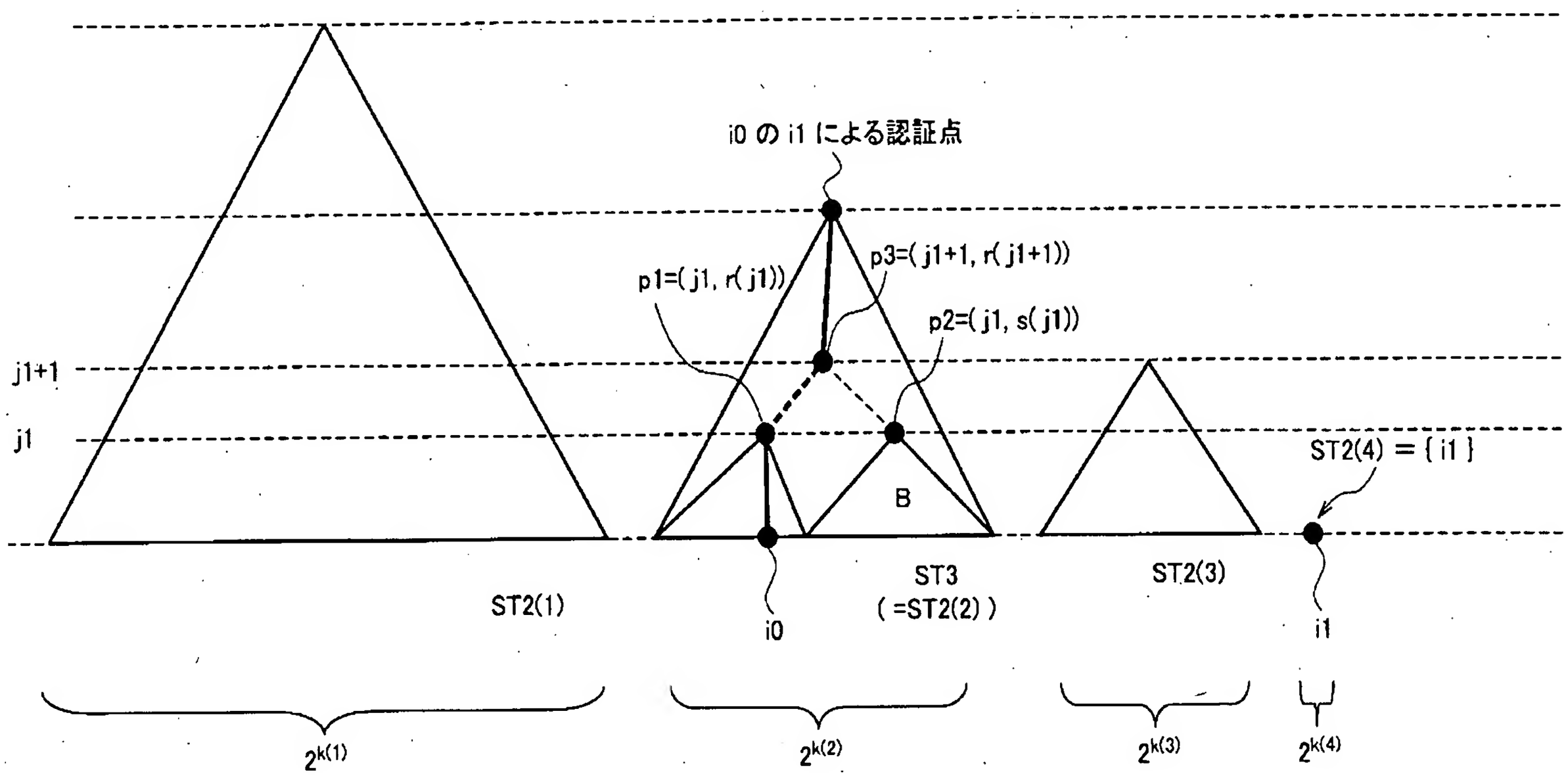
【図５０】

i0 と i1 がi1時点における1つの順次集約小木に属するとき



【図５１】

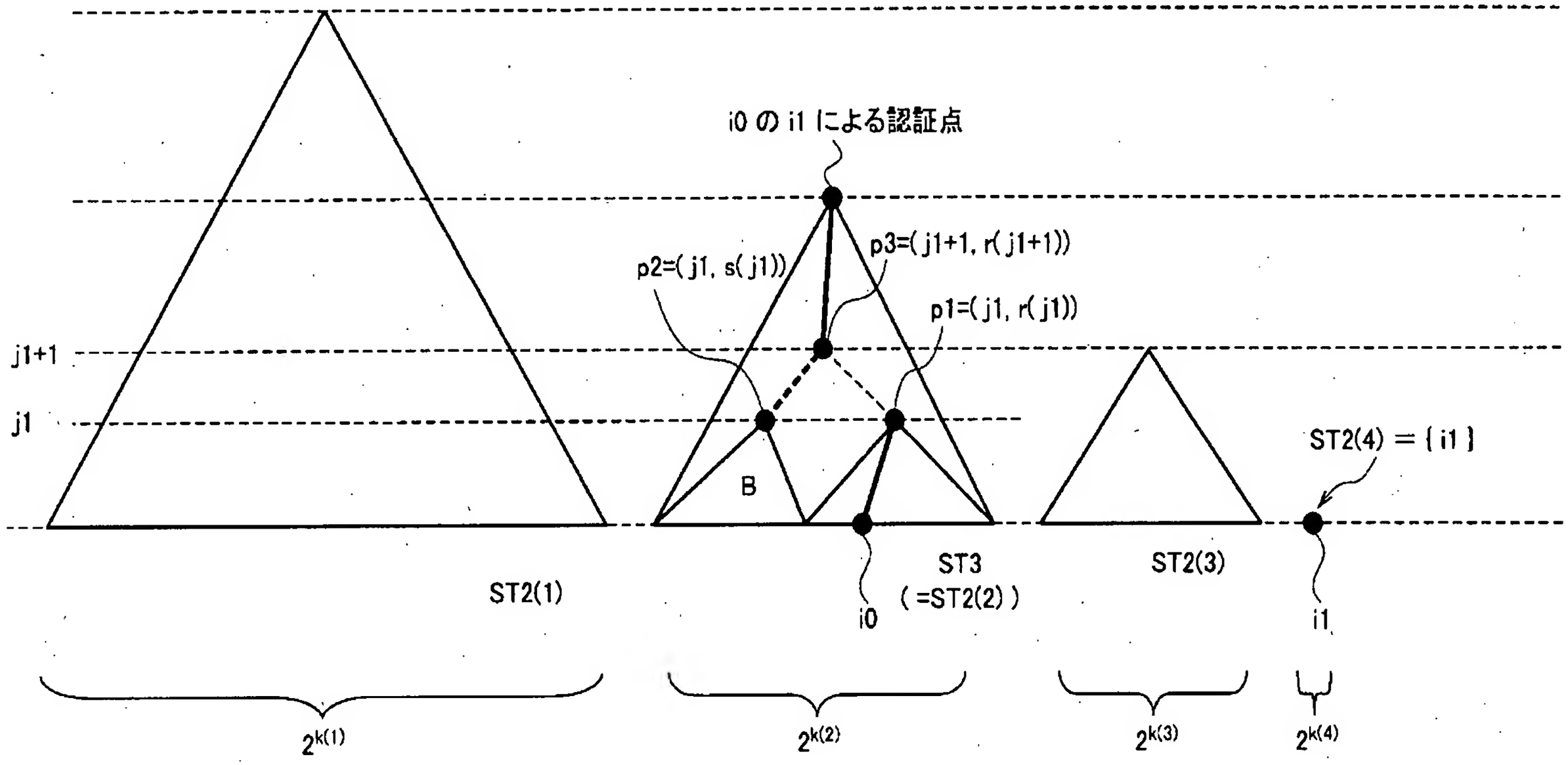
i0 と i1 がi1時点における1つの順次集約小木に属さないとき



$k(1) > k(2) > k(3) > k(4) = 0$

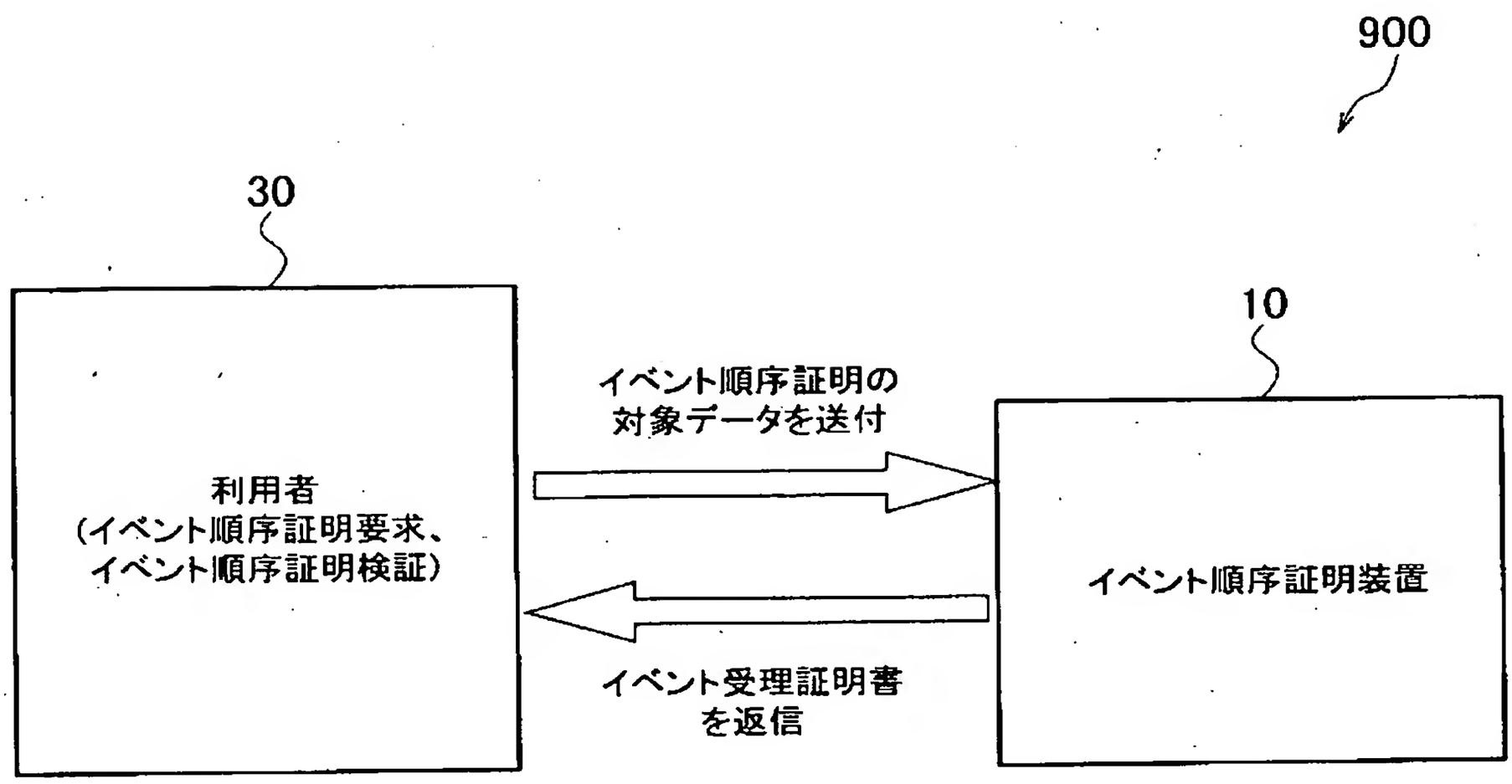
【図52】

i0 と i1 がi1時点における1つの順次集約小木に属さないとき

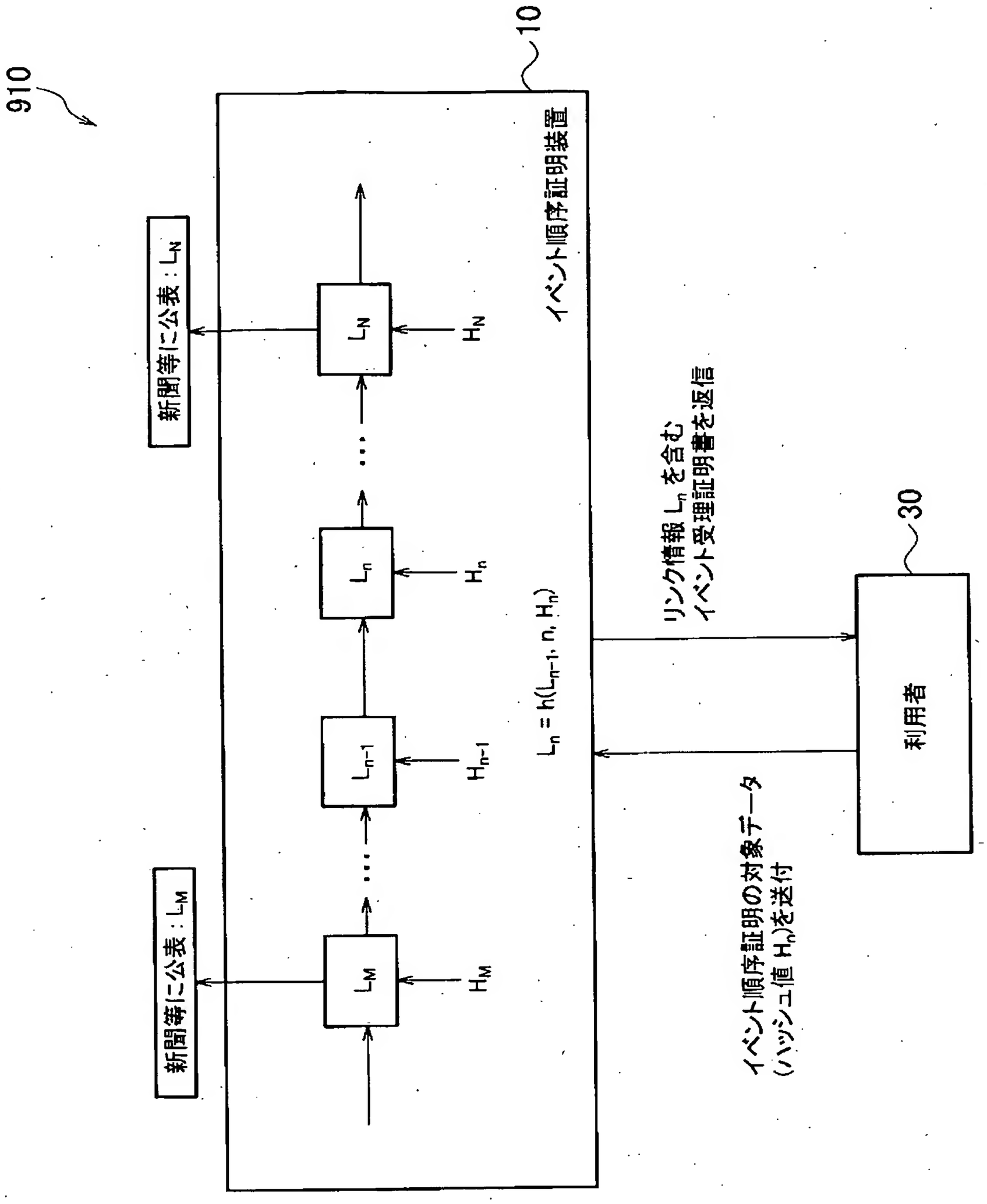


$k(1) > k(2) > k(3) > k(4) = 0$

【図５３】


900
30
利用者
（イベント順序証明要求、
イベント順序証明検証）
イベント順序証明の
対象データを送付
イベント受理証明書
を返信
10
イベント順序証明装置

【図５４】


910
10
イベント順序証明装置
新聞等に公表：L_N
L_N
H_N
新聞等に公表：L_M
L_M
H_M
L_{n-1}
H_{n-1}
L_n
H_n
$L_n = h(L_{n-1}, n, H_n)$
リンク情報 L_n を含む
イベント受理証明書を返信
イベント順序証明の対象データ
（ハッシュ値 H_n）を送付
30
利用者

【書類名】要約書
【要約】
【課題】木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、イベント順序証明要求をまとめた公表データを用いなくても、証明機関から発行されたイベント順序受理証明書の検証を行うことができる。
【解決手段】イベント順序証明システム100は、イベント順序証明装置1、複数のイベント順序証明利用者装置21、及び、以上の各装置を相互に接続するコンピュータネットワーク3を備えており、証明装置1が利用者装置21からのイベント順序証明要求に応えて、イベント順序受理証明書を含むイベント順序証明応答を利用者装置21に返信する。ここで、イベント順序証明応答は、シーケンス補完方式（登録点の即時補完データ及び該登録点より前に登録された各登録点の登録点における遅延補完データを証明応答に含む）による証明応答であり、利用者装置21は、証明装置1から受け取ったこの複数の証明応答から受理証明書の正当性を検証する。
【選択図】図1

出願人履歴

０００００４２２６
19990715
住所変更
５９１０２９２８６

東京都千代田区大手町二丁目３番１号
日本電信電話株式会社